Espacenet

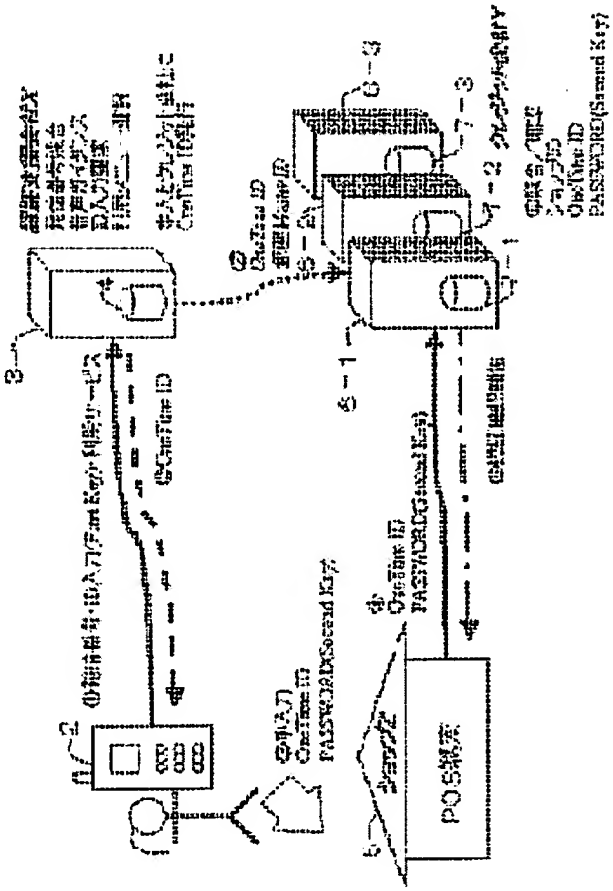
Bibliographic data: JP 2003323408 (A)

PERSONAL AUTHENTICATION METHOD AND SYSTEM

Publication date:	2003-11-14
Inventor(s):	ITOI MASAYUKI; TAKAGAWA TOMOKAZU +
Applicant(s):	ITOI MASAYUKI; TAKAGAWA TOMOKAZU +
Classification:	- **international:** ***G06F21/20; G06Q20/00; G07C9/00;*** (IPC1-7): G06F15/00; G06F17/60 - **European:** G06Q20/00K2B; G07C9/00B2
Application number:	JP20020126933 20020426
Priority number(s):	JP20020126933 20020426
Also published as:	• JP 3678417 (B2) • US 2003204725 (A1)

Abstract of JP 2003323408 (A)

PROBLEM TO BE SOLVED: To provide a low-cost, reliable personal authentication method enabling individual identification. ; SOLUTION: A membership ID of a user 1 is separately secretly managed by an authentication support company X, while the password by a credit company Y. The user 1 transmits the membership ID to the authentication support company X via a portable telephone 2, and the company X performs first step personal authentication, using the station serial number and the membership ID. If the authentication succeeds, the authentication support company X issues a one-time ID to the user 1 and notifies the credit company Y of it. The user 1 transmits the one-time ID and the password to the credit company Y from a shop Z. The credit company Y performs second step personal authentication, using the one-time ID and the password, and if it succeeds, the company Y supplies a service such as credit settlement. ; COPYRIGHT: (C)2004,JPO



Last updated: 26.04.2011 Worldwide Database 5.7.22; 92p

US 20030204725A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0204725 A1**

Itoi et al. (43) **Pub. Date: Oct. 30, 2003**

(54) **METHOD AND SYSTEM FOR VERIFYING IDENTITY**

(76) Inventors: **Masayuki Itoi**, Tokyo (JP); **Tomokazu Takagawa**, Kanagawa (JP)

Correspondence Address:
GALLAGHER & LATHROP, A PROFESSIONAL CORPORATION
601 CALIFORNIA ST
SUITE 1111
SAN FRANCISCO, CA 94108 (US)

(21) Appl. No.: **10/284,799**

(22) Filed: **Oct. 30, 2002**

(30) **Foreign Application Priority Data**

Apr. 26, 2002 (JP) 2002-126933

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**; G06F 17/60

(52) **U.S. Cl.** **713/168**; 705/64

(57) **ABSTRACT**

Verification facilitating company or companies X and verifying company or companies (e.g., credit service company or companies) Y may respectively manage member ID(s) and password(s) of user(s) **1** in mutually separate and mutually secret fashion. User(s) **1** may send member ID(s) to verification facilitating company or companies X from mobile telephone(s) **2**, and verification facilitating company or companies X may use originating telephone number(s) and/or member ID(s) to carry out first-stage identity check(s). In the event of positive verification of identity as a result of such identity check(s), verification facilitating company or companies X may issue one-time ID(s) to user(s) **1** and may communicate such one-time ID(s) to verifying company or companies (e.g., credit service company or companies) Y. User(s) **1** may send one-time ID(s) and password(s) to verifying company or companies (e.g., credit service company or companies) Y from company or companies (e.g., store or stores) Z. Verifying company or companies (e.g., credit service company or companies) Y may use one-time ID(s) and password(s) to carry out second-stage identity check(s), and in the event of positive verification of identity as a result of such identity check(s), may provide credit transaction processing or other such service(s).

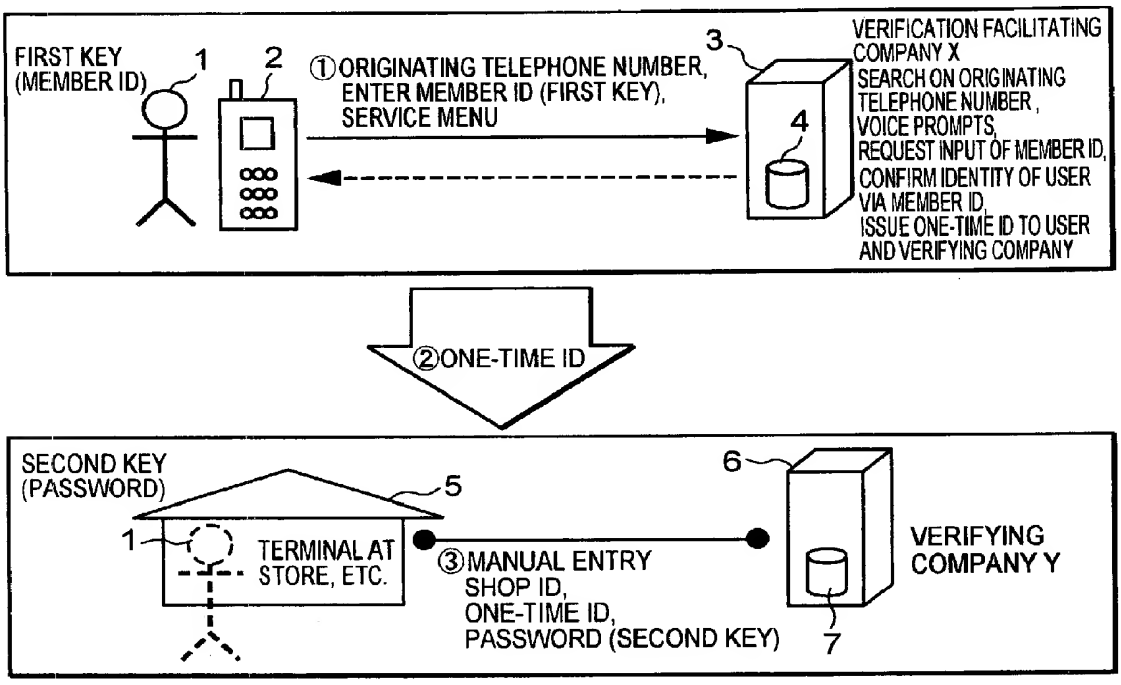


FIG. 1

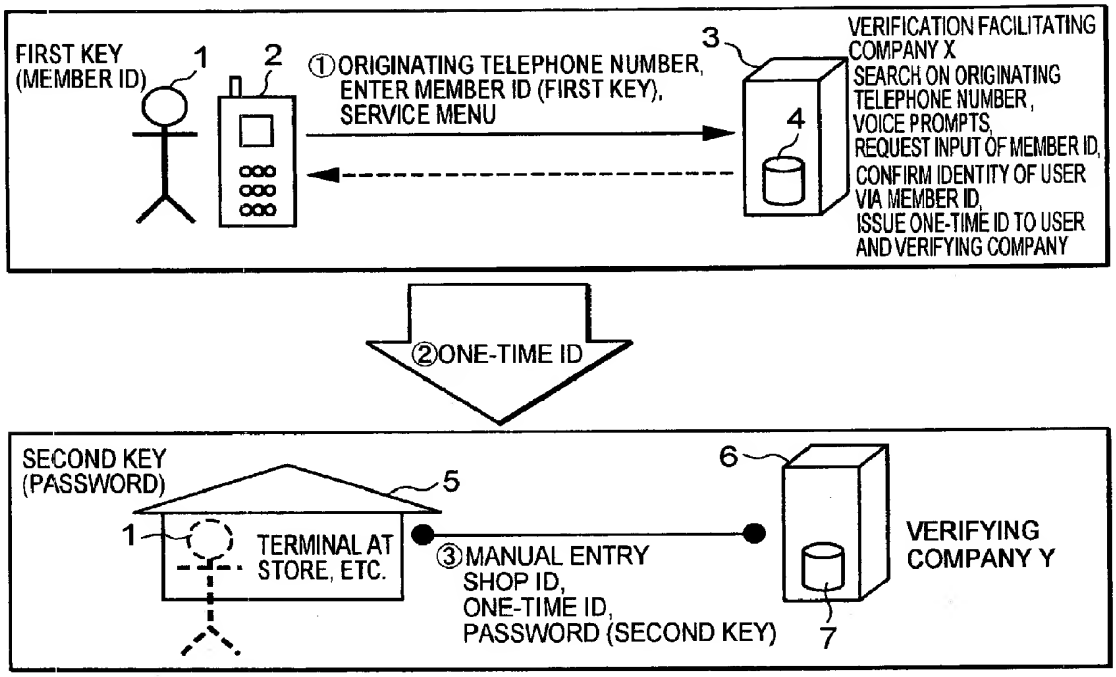

FIRST KEY
(MEMBER ID)
1
2
①ORIGINATING TELEPHONE NUMBER,
ENTER MEMBER ID (FIRST KEY),
SERVICE MENU
3
4
VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER,
VOICE PROMPTS,
REQUEST INPUT OF MEMBER ID,
CONFIRM IDENTITY OF USER VIA MEMBER ID,
ISSUE ONE-TIME ID TO USER AND VERIFYING COMPANY
②ONE-TIME ID
SECOND KEY
(PASSWORD)
5
1
TERMINAL AT STORE, ETC.
③MANUAL ENTRY
SHOP ID,
ONE-TIME ID,
PASSWORD (SECOND KEY)
6
7
VERIFYING COMPANY Y

FIG. 2

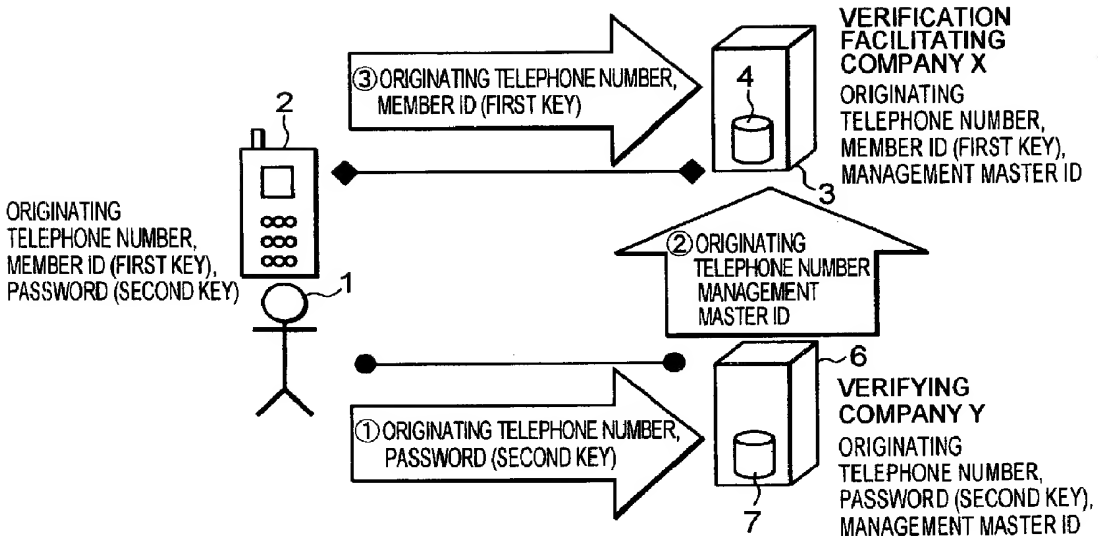

VERIFICATION FACILITATING COMPANY X
ORIGINATING TELEPHONE NUMBER, MEMBER ID (FIRST KEY), MANAGEMENT MASTER ID
③ORIGINATING TELEPHONE NUMBER, MEMBER ID (FIRST KEY)
②ORIGINATING TELEPHONE NUMBER MANAGEMENT MASTER ID
①ORIGINATING TELEPHONE NUMBER, PASSWORD (SECOND KEY)
ORIGINATING TELEPHONE NUMBER, MEMBER ID (FIRST KEY), PASSWORD (SECOND KEY)
VERIFYING COMPANY Y
ORIGINATING TELEPHONE NUMBER, PASSWORD (SECOND KEY), MANAGEMENT MASTER ID
1
2
3
4
6
7

FIG. 3

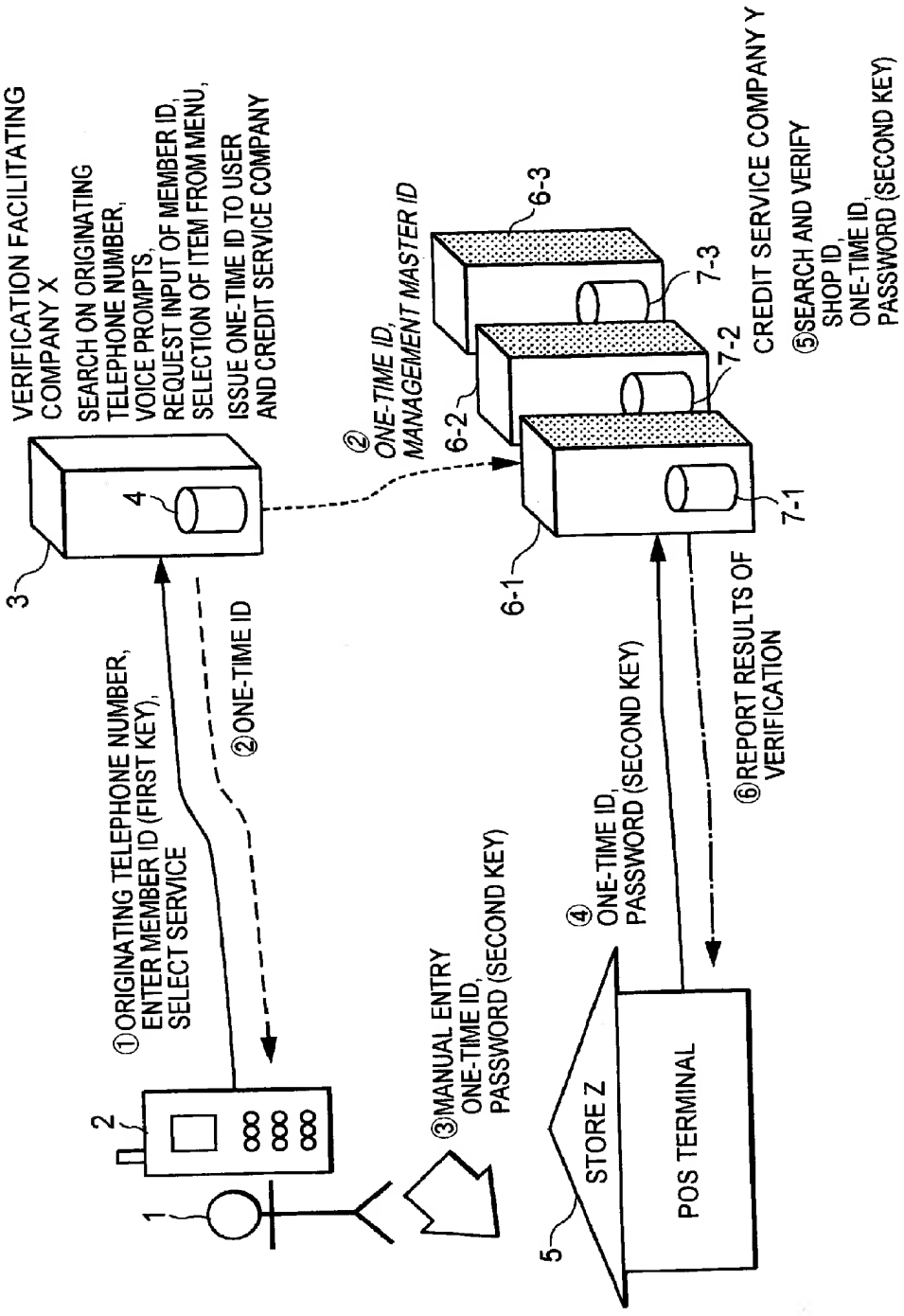

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU, ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
② ONE-TIME ID, MANAGEMENT MASTER ID
CREDIT SERVICE COMPANY Y
⑤SEARCH AND VERIFY SHOP ID, ONE-TIME ID, PASSWORD (SECOND KEY)
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
②ONE-TIME ID
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
④ ONE-TIME ID, PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
STORE Z
POS TERMINAL
1
2
3
4
5
6-1
6-2
6-3
7-1
7-2
7-3

FIG. 4

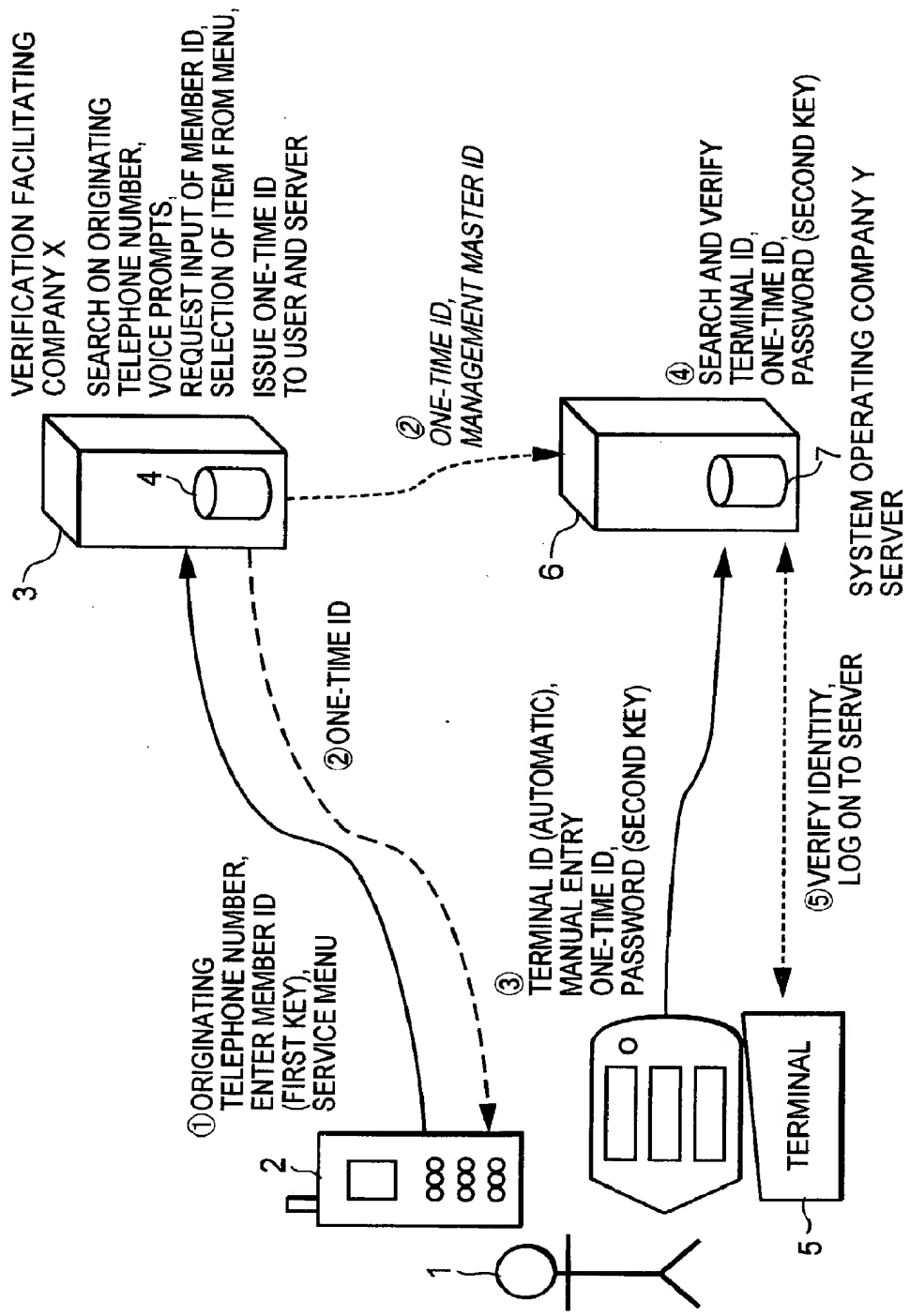

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND SERVER
② ONE-TIME ID, MANAGEMENT MASTER ID
④ SEARCH AND VERIFY TERMINAL ID, ONE-TIME ID, PASSWORD (SECOND KEY)
SYSTEM OPERATING COMPANY Y SERVER
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SERVICE MENU
②ONE-TIME ID
③ TERMINAL ID (AUTOMATIC), MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
⑤VERIFY IDENTITY, LOG ON TO SERVER
TERMINAL
1
2
3
4
5
6
7

FIG. 5

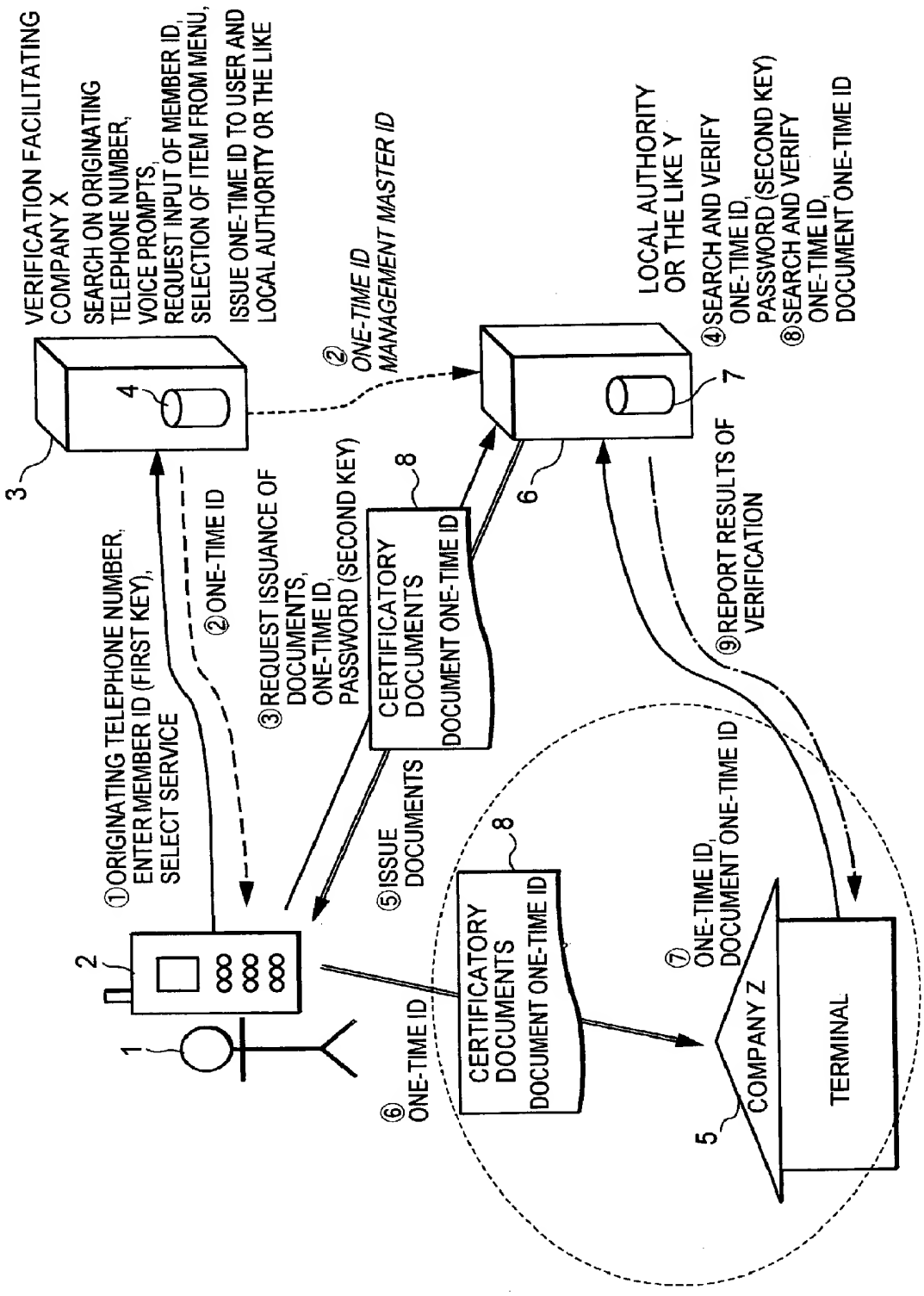

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND LOCAL AUTHORITY OR THE LIKE
② ONE-TIME ID MANAGEMENT MASTER ID
LOCAL AUTHORITY OR THE LIKE Y
④SEARCH AND VERIFY ONE-TIME ID, PASSWORD (SECOND KEY)
⑧SEARCH AND VERIFY ONE-TIME ID, DOCUMENT ONE-TIME ID
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
②ONE-TIME ID
③REQUEST ISSUANCE OF DOCUMENTS, ONE-TIME ID, PASSWORD (SECOND KEY)
CERTIFICATORY DOCUMENTS
DOCUMENT ONE-TIME ID
⑤ISSUE DOCUMENTS
⑨REPORT RESULTS OF VERIFICATION
⑥ONE-TIME ID
CERTIFICATORY DOCUMENTS
DOCUMENT ONE-TIME ID
⑦ONE-TIME ID, DOCUMENT ONE-TIME ID
COMPANY Z
TERMINAL
1
2
3
4
5
6
7
8
8

FIG. 6

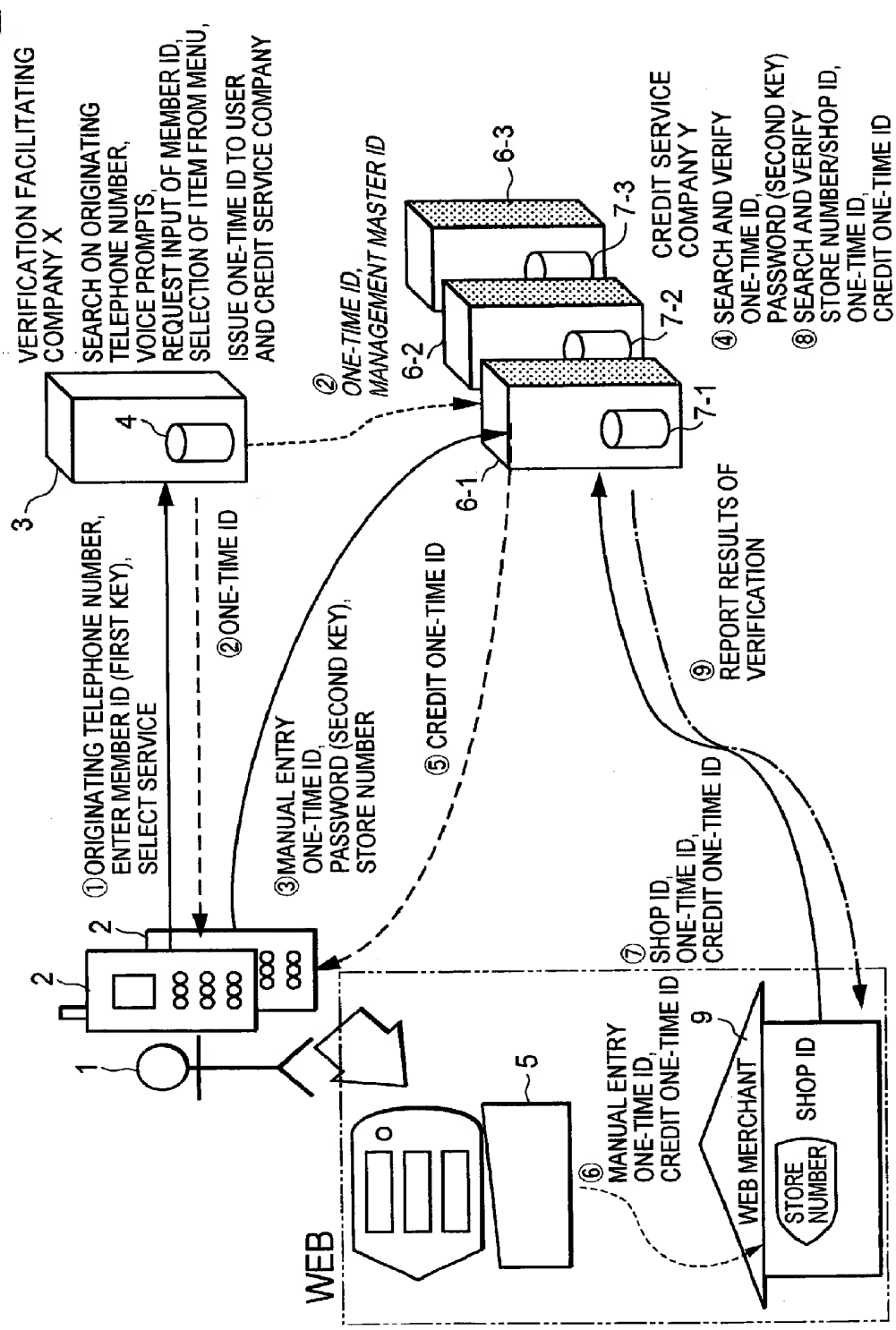

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
② ONE-TIME ID, MANAGEMENT MASTER ID
CREDIT SERVICE COMPANY Y
④ SEARCH AND VERIFY ONE-TIME ID, PASSWORD (SECOND KEY)
⑧ SEARCH AND VERIFY STORE NUMBER/SHOP ID, ONE-TIME ID, CREDIT ONE-TIME ID
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
②ONE-TIME ID
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY), STORE NUMBER
⑤ CREDIT ONE-TIME ID
⑨ REPORT RESULTS OF VERIFICATION
⑦ SHOP ID, ONE-TIME ID, CREDIT ONE-TIME ID
⑥ MANUAL ENTRY ONE-TIME ID, CREDIT ONE-TIME ID
WEB MERCHANT
SHOP ID
STORE NUMBER
WEB

FIG. 7

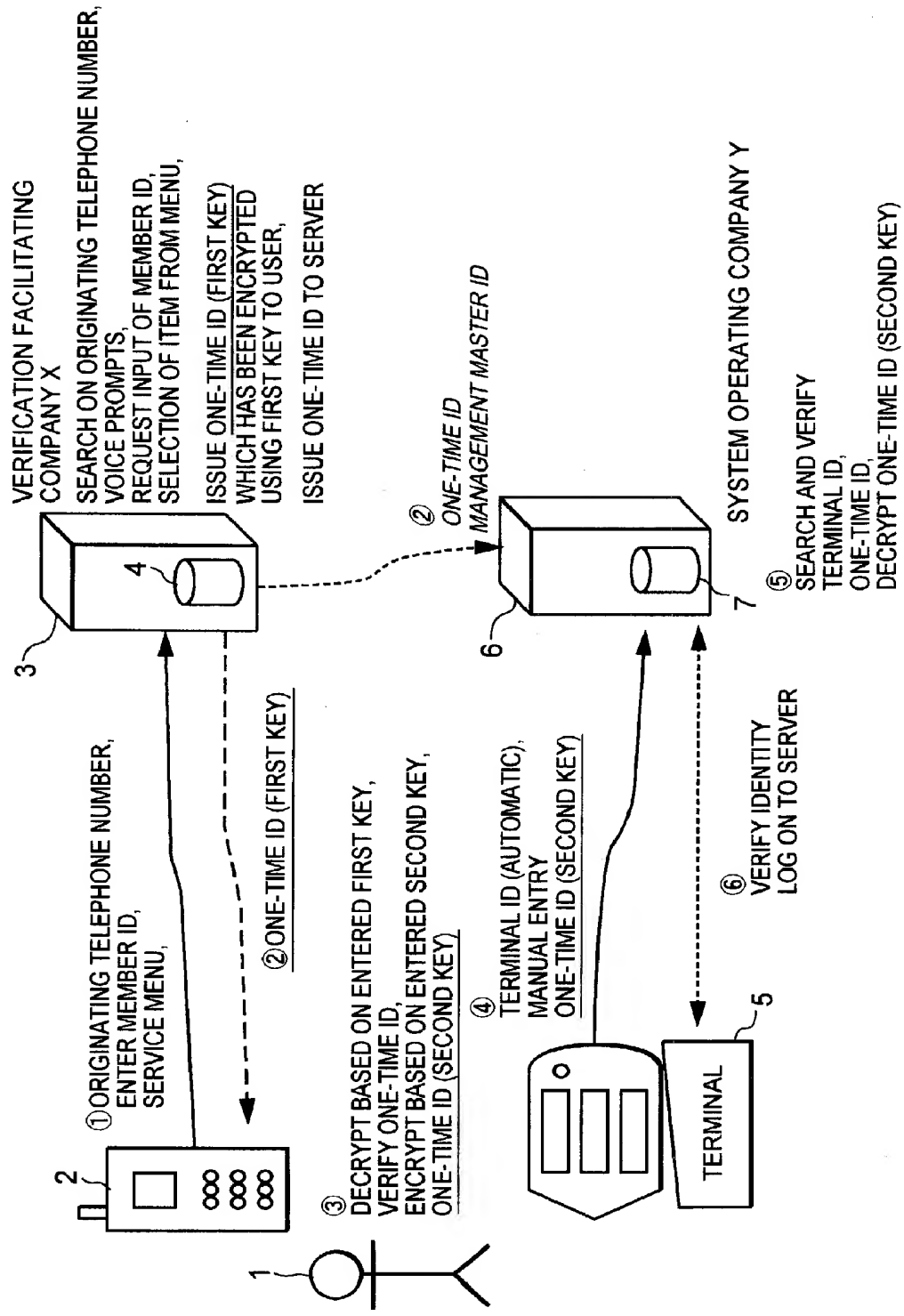

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID (FIRST KEY) WHICH HAS BEEN ENCRYPTED USING FIRST KEY TO USER,
ISSUE ONE-TIME ID TO SERVER
② ONE-TIME ID MANAGEMENT MASTER ID
SYSTEM OPERATING COMPANY Y
⑤ SEARCH AND VERIFY TERMINAL ID, ONE-TIME ID, DECRYPT ONE-TIME ID (SECOND KEY)
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID, SERVICE MENU,
②ONE-TIME ID (FIRST KEY)
③ DECRYPT BASED ON ENTERED FIRST KEY, VERIFY ONE-TIME ID, ENCRYPT BASED ON ENTERED SECOND KEY, ONE-TIME ID (SECOND KEY)
④ TERMINAL ID (AUTOMATIC), MANUAL ENTRY ONE-TIME ID (SECOND KEY)
⑥ VERIFY IDENTITY LOG ON TO SERVER
TERMINAL
1
2
3
4
5
6
7

FIG. 8

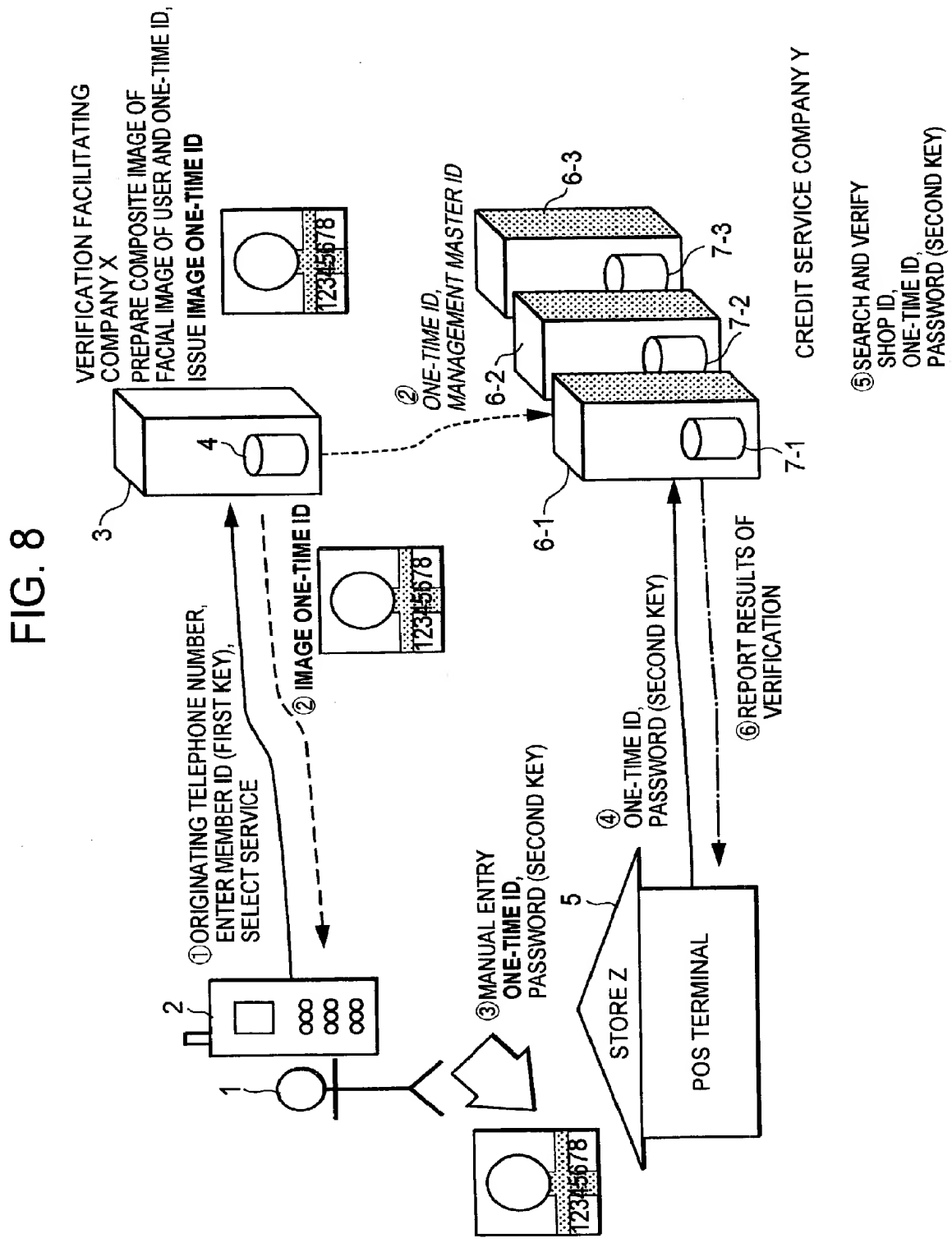

VERIFICATION FACILITATING COMPANY X
PREPARE COMPOSITE IMAGE OF FACIAL IMAGE OF USER AND ONE-TIME ID,
ISSUE IMAGE ONE-TIME ID
CREDIT SERVICE COMPANY Y
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
② IMAGE ONE-TIME ID
② ONE-TIME ID, MANAGEMENT MASTER ID
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
④ ONE-TIME ID, PASSWORD (SECOND KEY)
⑤SEARCH AND VERIFY SHOP ID, ONE-TIME ID, PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
STORE Z
POS TERMINAL
12345678
1
2
3
4
5
6-1
6-2
6-3
7-1
7-2
7-3

FIG. 9

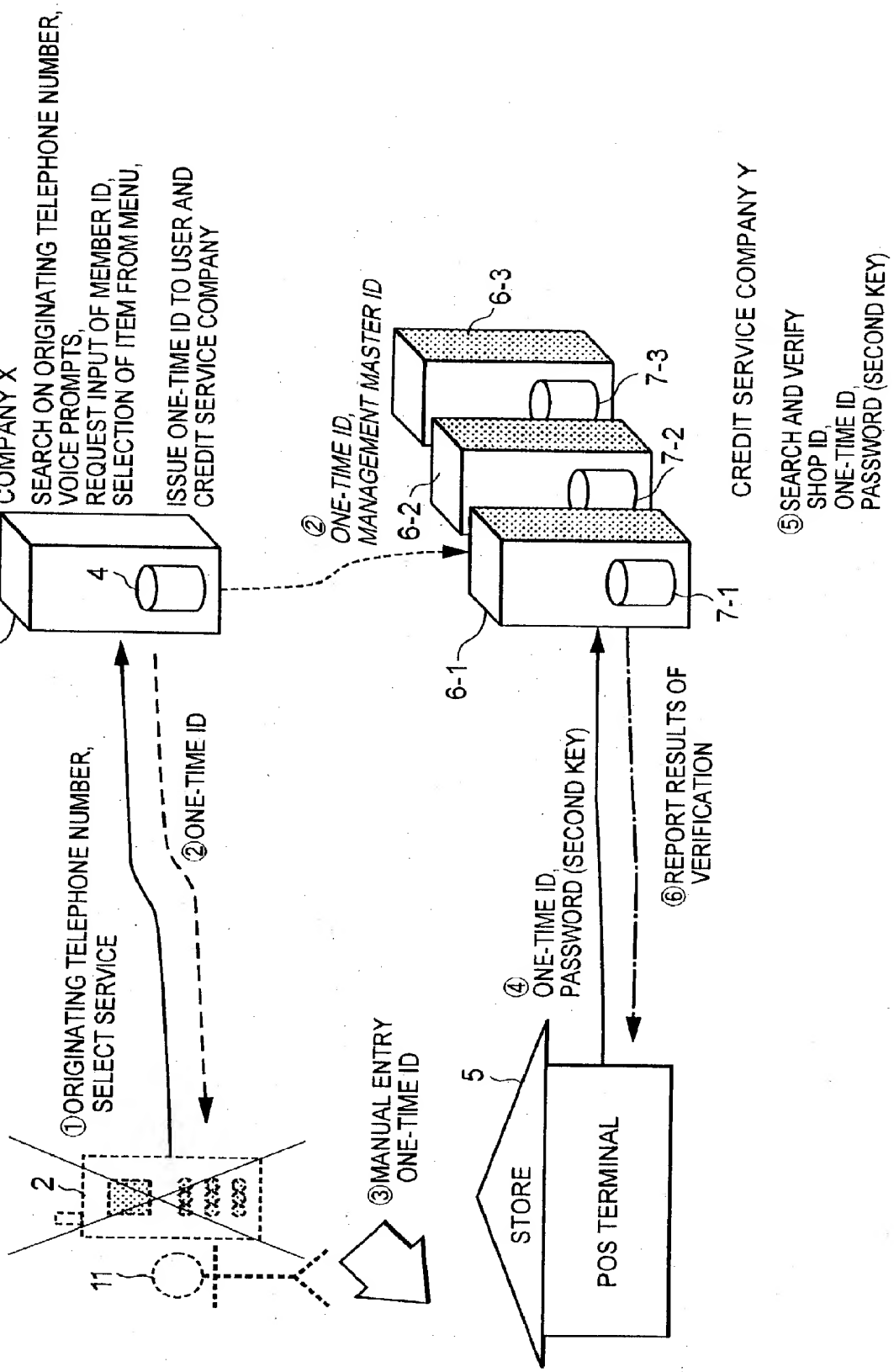

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER,
VOICE PROMPTS,
REQUEST INPUT OF MEMBER ID,
SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
3
4
② ONE-TIME ID, MANAGEMENT MASTER ID
6-1
6-2
6-3
7-1
7-2
7-3
CREDIT SERVICE COMPANY Y
⑤SEARCH AND VERIFY
SHOP ID,
ONE-TIME ID,
PASSWORD (SECOND KEY)
①ORIGINATING TELEPHONE NUMBER, SELECT SERVICE
②ONE-TIME ID
③MANUAL ENTRY ONE-TIME ID
④ ONE-TIME ID, PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
2
11
5
STORE
POS TERMINAL

FIG. 10

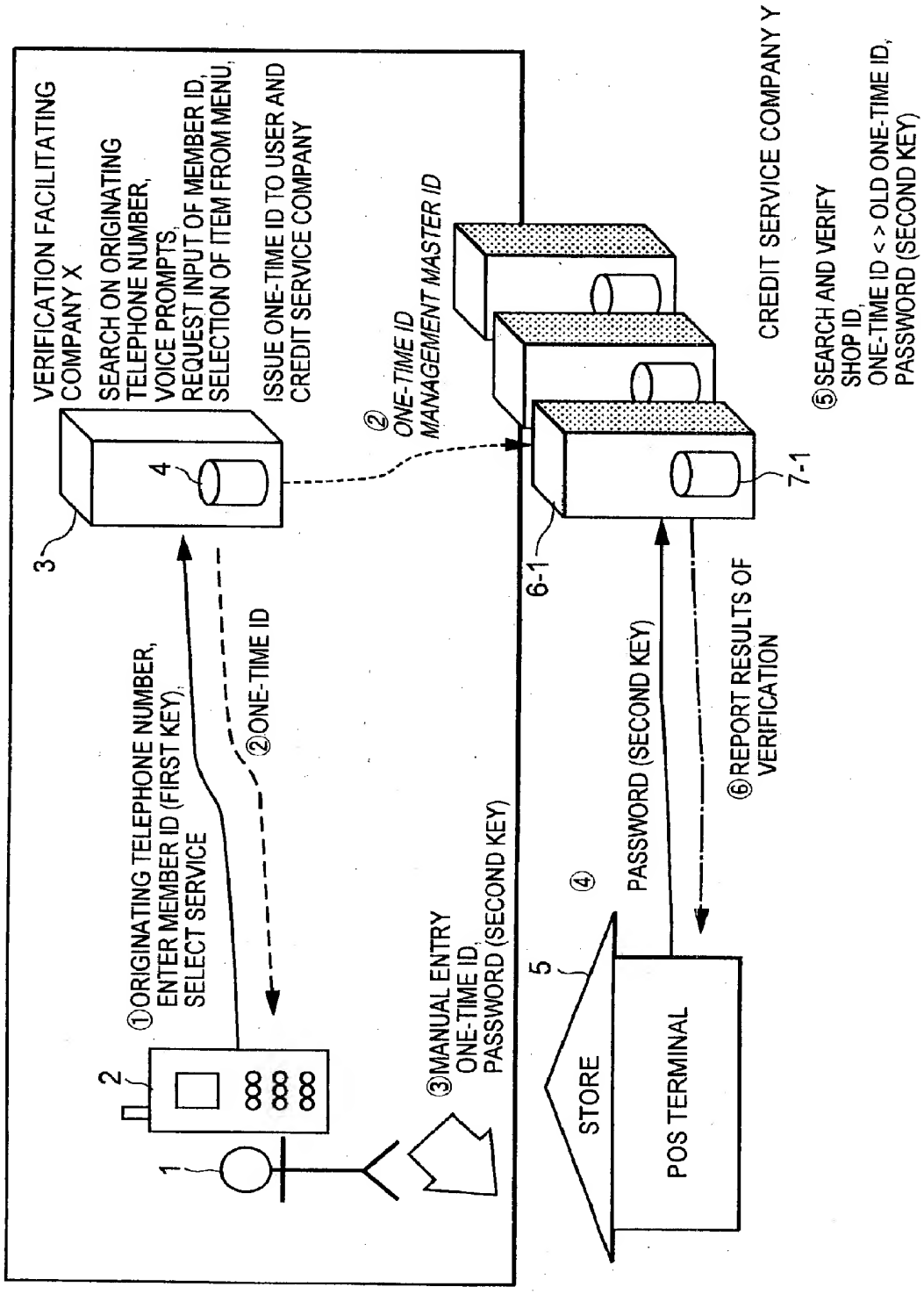

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
② ONE-TIME ID MANAGEMENT MASTER ID
CREDIT SERVICE COMPANY Y
⑤SEARCH AND VERIFY SHOP ID, ONE-TIME ID < > OLD ONE-TIME ID, PASSWORD (SECOND KEY)
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
②ONE-TIME ID
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
④ PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
STORE
POS TERMINAL
1
2
3
4
5
6-1
7-1

FIG. 11

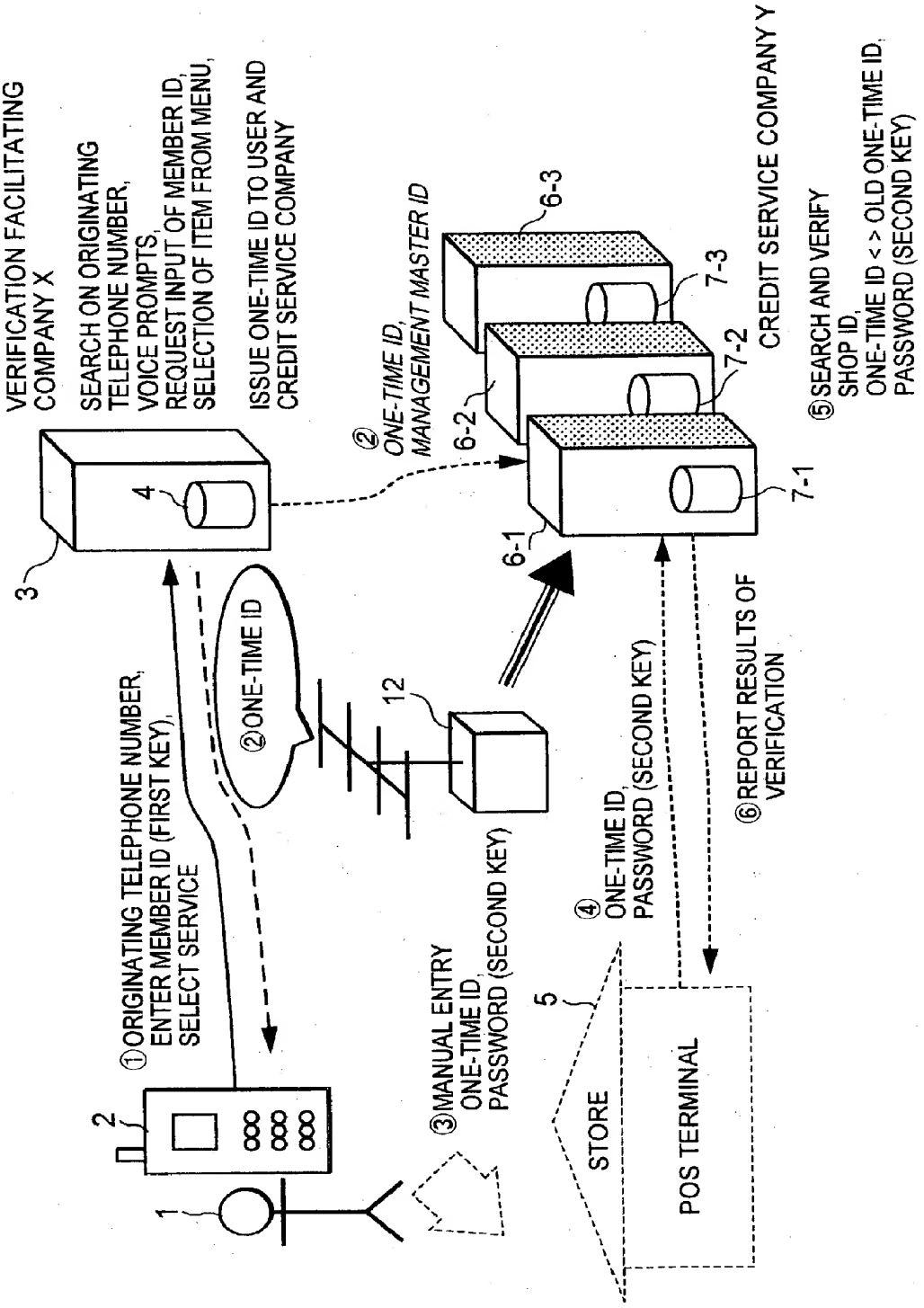

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
② ONE-TIME ID, MANAGEMENT MASTER ID
CREDIT SERVICE COMPANY Y
⑤SEARCH AND VERIFY SHOP ID, ONE-TIME ID < > OLD ONE-TIME ID, PASSWORD (SECOND KEY)
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
②ONE-TIME ID
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
④ ONE-TIME ID, PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
STORE
POS TERMINAL
1
2
3
4
5
6-1
6-2
6-3
7-1
7-2
7-3
12

FIG. 12

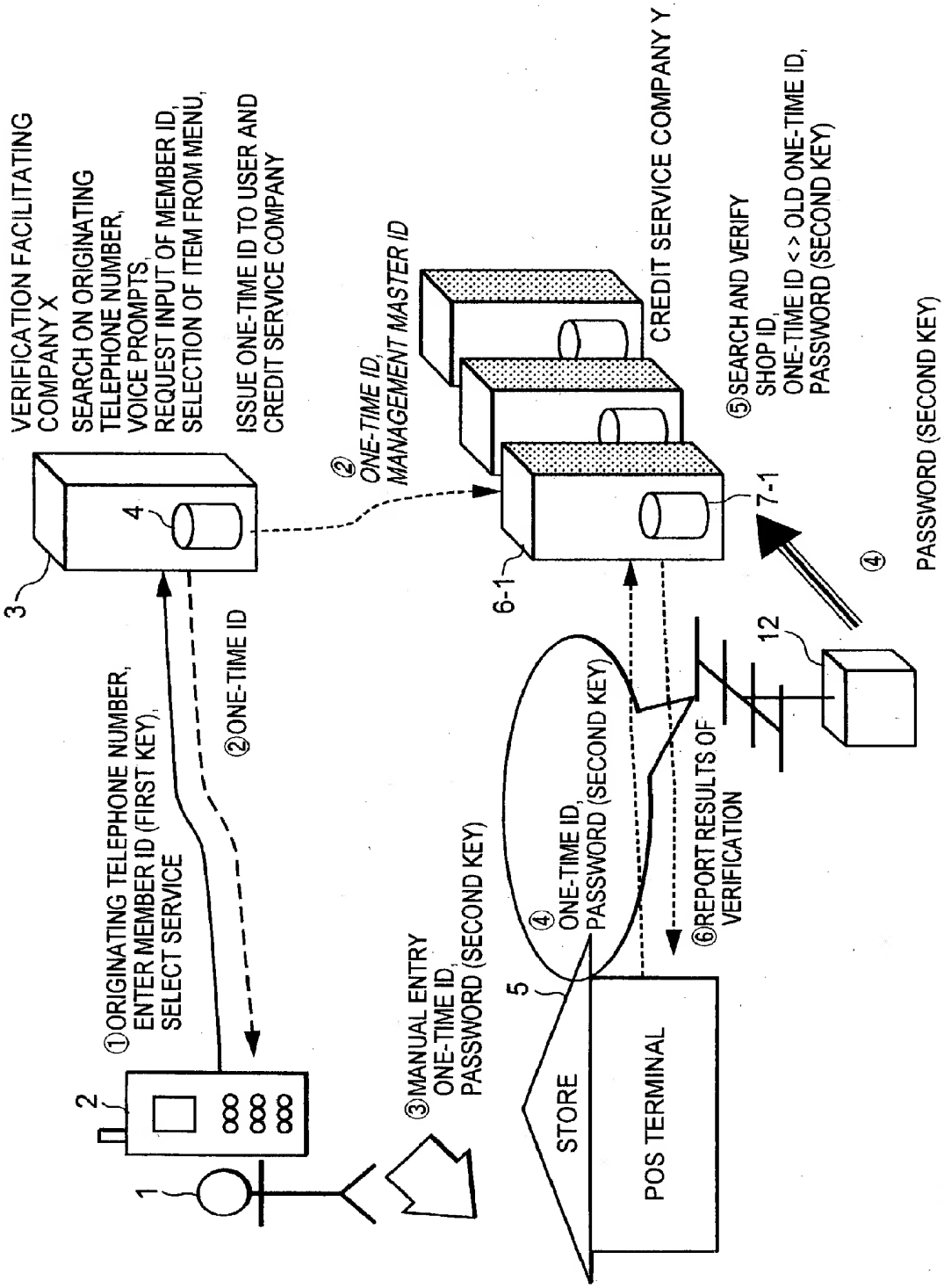

VERIFICATION FACILITATING COMPANY X
SEARCH ON ORIGINATING TELEPHONE NUMBER, VOICE PROMPTS, REQUEST INPUT OF MEMBER ID, SELECTION OF ITEM FROM MENU,
ISSUE ONE-TIME ID TO USER AND CREDIT SERVICE COMPANY
②ONE-TIME ID
①ORIGINATING TELEPHONE NUMBER, ENTER MEMBER ID (FIRST KEY), SELECT SERVICE
③MANUAL ENTRY ONE-TIME ID, PASSWORD (SECOND KEY)
② ONE-TIME ID, MANAGEMENT MASTER ID
CREDIT SERVICE COMPANY Y
⑤SEARCH AND VERIFY SHOP ID, ONE-TIME ID < > OLD ONE-TIME ID, PASSWORD (SECOND KEY)
④ PASSWORD (SECOND KEY)
④ ONE-TIME ID, PASSWORD (SECOND KEY)
⑥REPORT RESULTS OF VERIFICATION
STORE
POS TERMINAL
1
2
3
4
5
6-1
7-1
12

FIG. 13

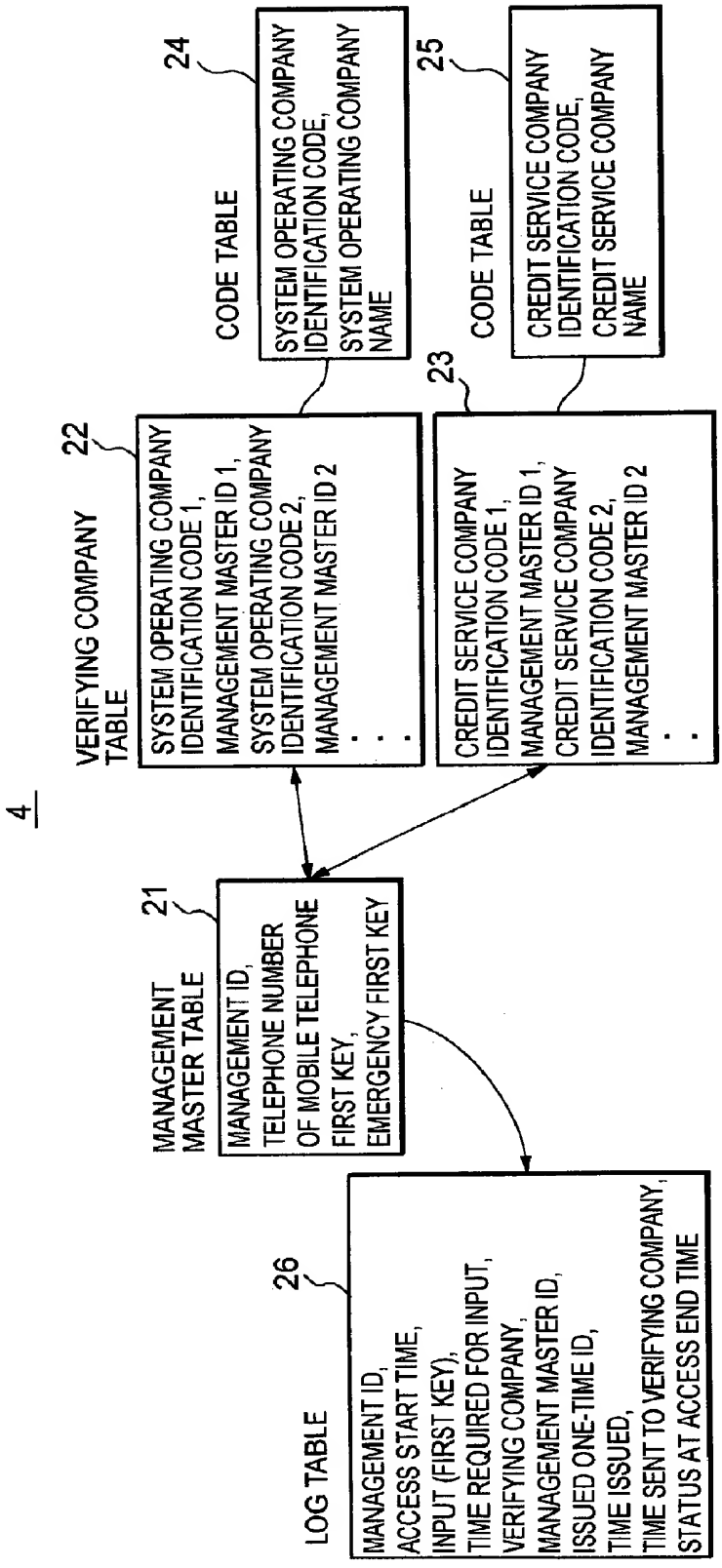

4
VERIFYING COMPANY TABLE
22
SYSTEM OPERATING COMPANY IDENTIFICATION CODE 1,
MANAGEMENT MASTER ID 1,
SYSTEM OPERATING COMPANY IDENTIFICATION CODE 2,
MANAGEMENT MASTER ID 2
. . .
CODE TABLE
24
SYSTEM OPERATING COMPANY IDENTIFICATION CODE,
SYSTEM OPERATING COMPANY NAME
23
CREDIT SERVICE COMPANY IDENTIFICATION CODE 1,
MANAGEMENT MASTER ID 1,
CREDIT SERVICE COMPANY IDENTIFICATION CODE 2,
MANAGEMENT MASTER ID 2
. . .
CODE TABLE
25
CREDIT SERVICE COMPANY IDENTIFICATION CODE,
CREDIT SERVICE COMPANY NAME
MANAGEMENT MASTER TABLE
21
MANAGEMENT ID,
TELEPHONE NUMBER OF MOBILE TELEPHONE
FIRST KEY,
EMERGENCY FIRST KEY
LOG TABLE
26
MANAGEMENT ID,
ACCESS START TIME,
INPUT (FIRST KEY),
TIME REQUIRED FOR INPUT,
VERIFYING COMPANY,
MANAGEMENT MASTER ID,
ISSUED ONE-TIME ID,
TIME ISSUED,
TIME SENT TO VERIFYING COMPANY,
STATUS AT ACCESS END TIME

FIG. 14

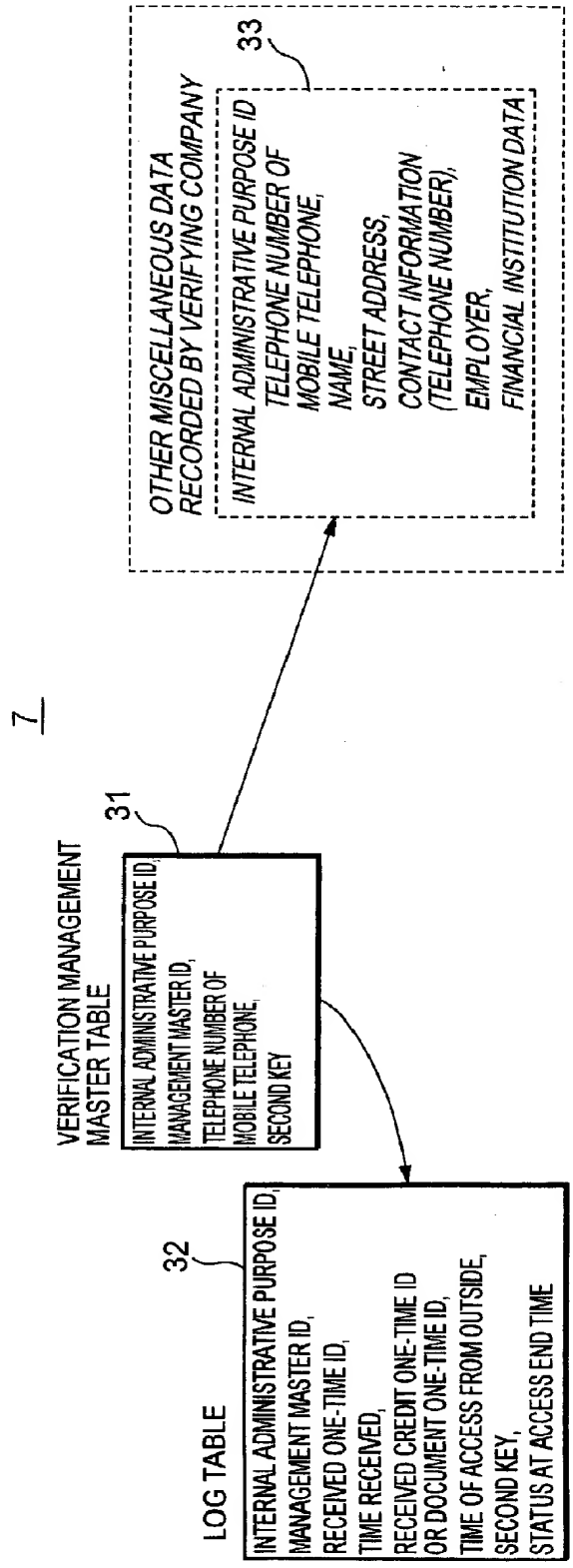

7
VERIFICATION MANAGEMENT MASTER TABLE
31
INTERNAL ADMINISTRATIVE PURPOSE ID,
MANAGEMENT MASTER ID,
TELEPHONE NUMBER OF MOBILE TELEPHONE,
SECOND KEY
OTHER MISCELLANEOUS DATA RECORDED BY VERIFYING COMPANY
33
INTERNAL ADMINISTRATIVE PURPOSE ID
TELEPHONE NUMBER OF MOBILE TELEPHONE,
NAME,
STREET ADDRESS,
CONTACT INFORMATION (TELEPHONE NUMBER),
EMPLOYER,
FINANCIAL INSTITUTION DATA
LOG TABLE
32
INTERNAL ADMINISTRATIVE PURPOSE ID,
MANAGEMENT MASTER ID,
RECEIVED ONE-TIME ID,
TIME RECEIVED,
RECEIVED CREDIT ONE-TIME ID OR DOCUMENT ONE-TIME ID,
TIME OF ACCESS FROM OUTSIDE,
SECOND KEY,
STATUS AT ACCESS END TIME

FIG. 15

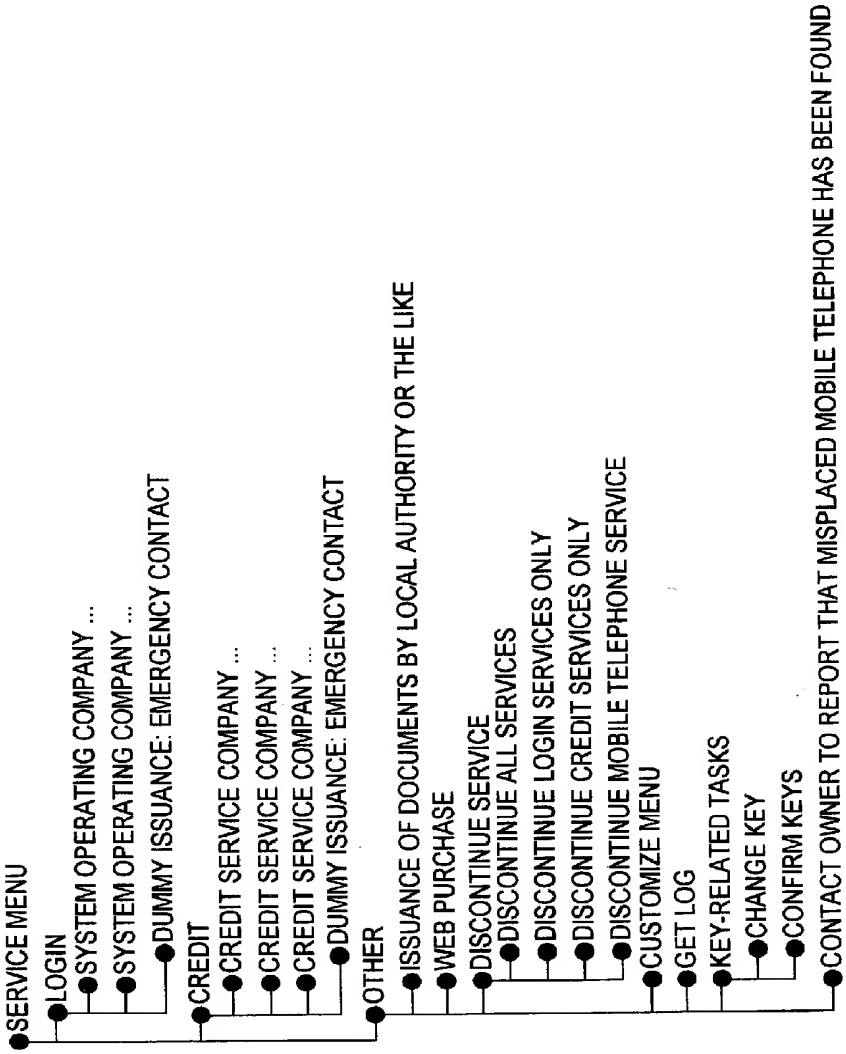

SERVICE MENU
LOGIN
SYSTEM OPERATING COMPANY ...
SYSTEM OPERATING COMPANY ...
DUMMY ISSUANCE: EMERGENCY CONTACT
CREDIT
CREDIT SERVICE COMPANY ...
CREDIT SERVICE COMPANY ...
CREDIT SERVICE COMPANY ...
DUMMY ISSUANCE: EMERGENCY CONTACT
OTHER
ISSUANCE OF DOCUMENTS BY LOCAL AUTHORITY OR THE LIKE
WEB PURCHASE
DISCONTINUE SERVICE
DISCONTINUE ALL SERVICES
DISCONTINUE LOGIN SERVICES ONLY
DISCONTINUE CREDIT SERVICES ONLY
DISCONTINUE MOBILE TELEPHONE SERVICE
CUSTOMIZE MENU
GET LOG
KEY-RELATED TASKS
CHANGE KEY
CONFIRM KEYS
CONTACT OWNER TO REPORT THAT MISPLACED MOBILE TELEPHONE HAS BEEN FOUND

FIG. 16

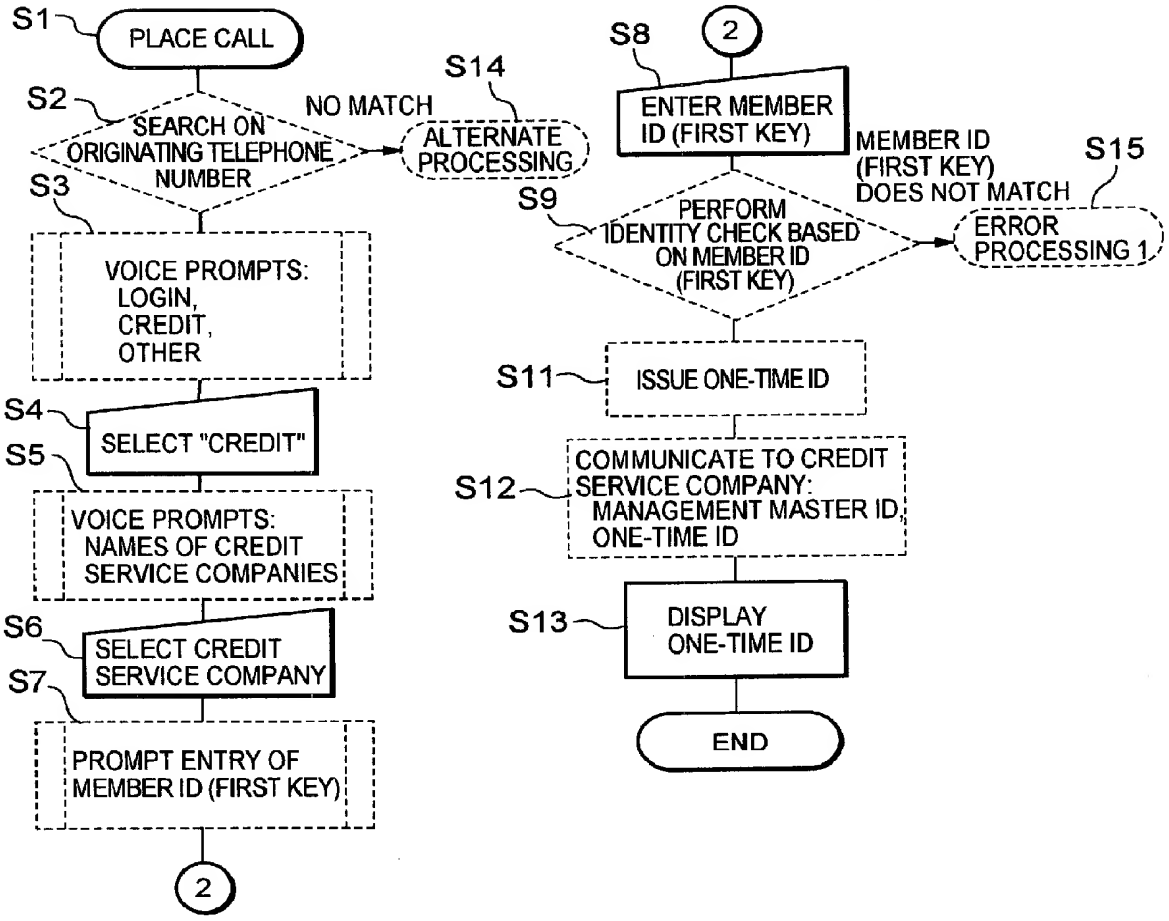

S1
PLACE CALL
S2
SEARCH ON ORIGINATING TELEPHONE NUMBER
NO MATCH
S14
ALTERNATE PROCESSING
S3
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S4
SELECT "CREDIT"
S5
VOICE PROMPTS: NAMES OF CREDIT SERVICE COMPANIES
S6
SELECT CREDIT SERVICE COMPANY
S7
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
2
S8
2
ENTER MEMBER ID (FIRST KEY)
S9
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
MEMBER ID (FIRST KEY) DOES NOT MATCH
S15
ERROR PROCESSING 1
S11
ISSUE ONE-TIME ID
S12
COMMUNICATE TO CREDIT SERVICE COMPANY: MANAGEMENT MASTER ID, ONE-TIME ID
S13
DISPLAY ONE-TIME ID
END

FIG. 17

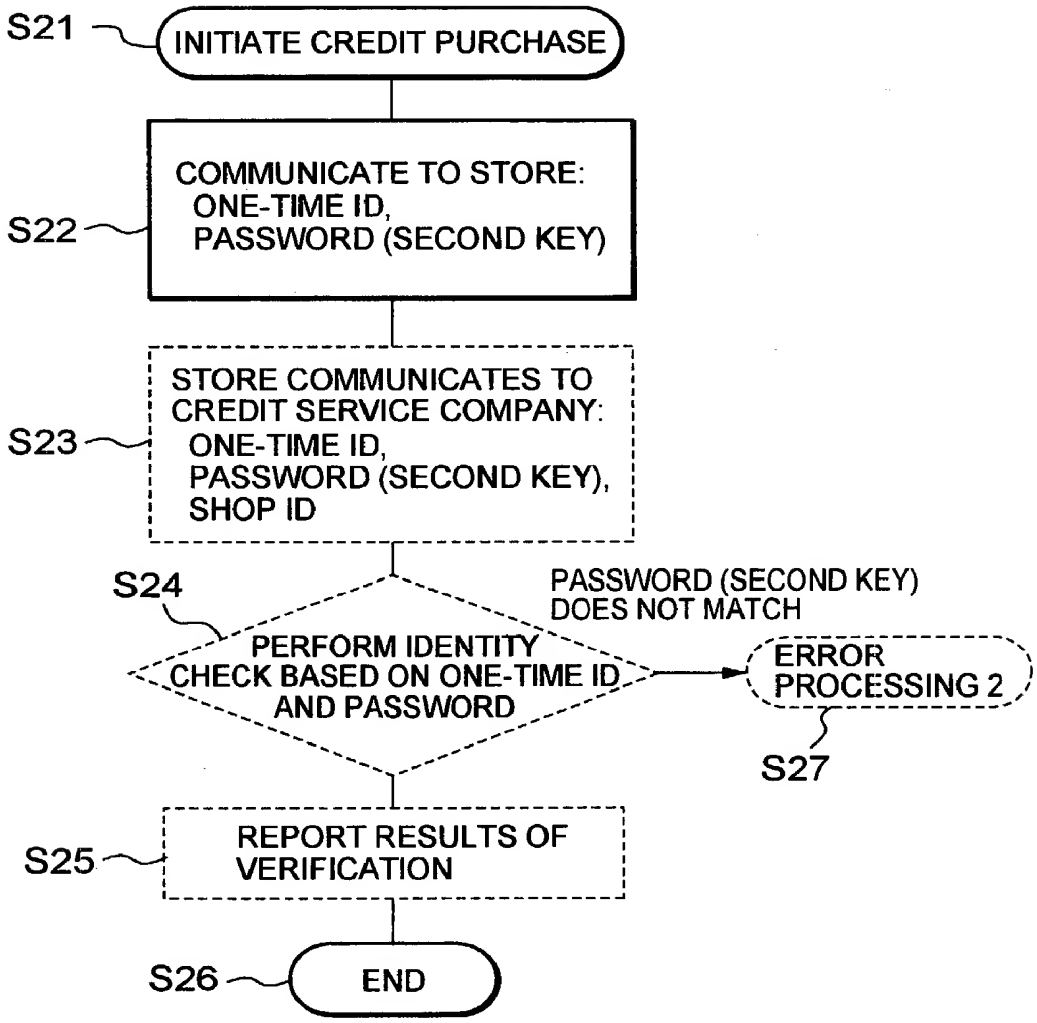

S21
INITIATE CREDIT PURCHASE
S22
COMMUNICATE TO STORE:
ONE-TIME ID,
PASSWORD (SECOND KEY)
S23
STORE COMMUNICATES TO
CREDIT SERVICE COMPANY:
ONE-TIME ID,
PASSWORD (SECOND KEY),
SHOP ID
S24
PERFORM IDENTITY
CHECK BASED ON ONE-TIME ID
AND PASSWORD
PASSWORD (SECOND KEY)
DOES NOT MATCH
ERROR
PROCESSING 2
S27
S25
REPORT RESULTS OF
VERIFICATION
S26
END

FIG.18

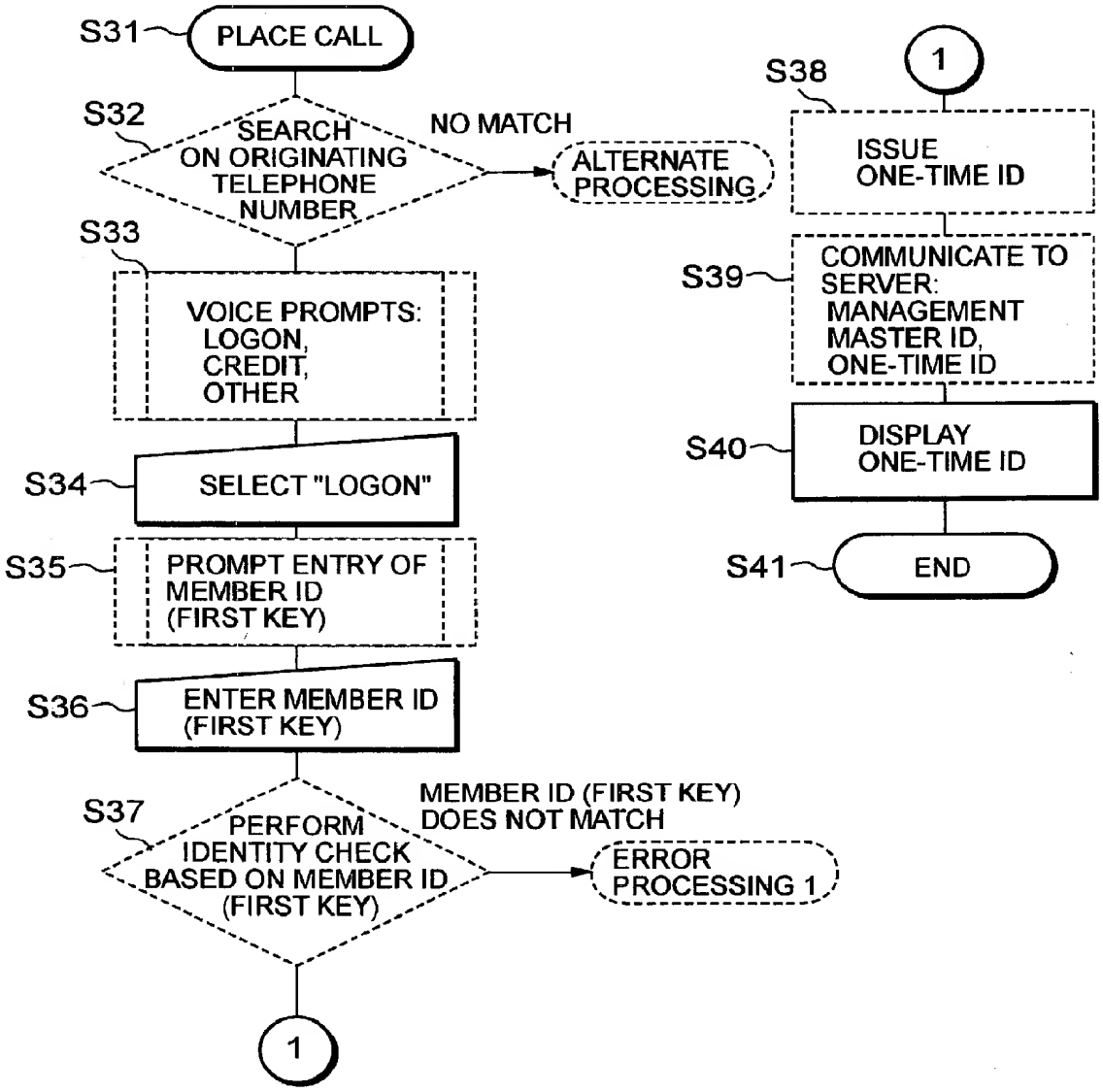

S31
PLACE CALL
S32
SEARCH ON ORIGINATING TELEPHONE NUMBER
NO MATCH
ALTERNATE PROCESSING
S33
VOICE PROMPTS: LOGON, CREDIT, OTHER
S34
SELECT "LOGON"
S35
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S36
ENTER MEMBER ID (FIRST KEY)
S37
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1
1
1
S38
ISSUE ONE-TIME ID
S39
COMMUNICATE TO SERVER: MANAGEMENT MASTER ID, ONE-TIME ID
S40
DISPLAY ONE-TIME ID
S41
END

FIG.19

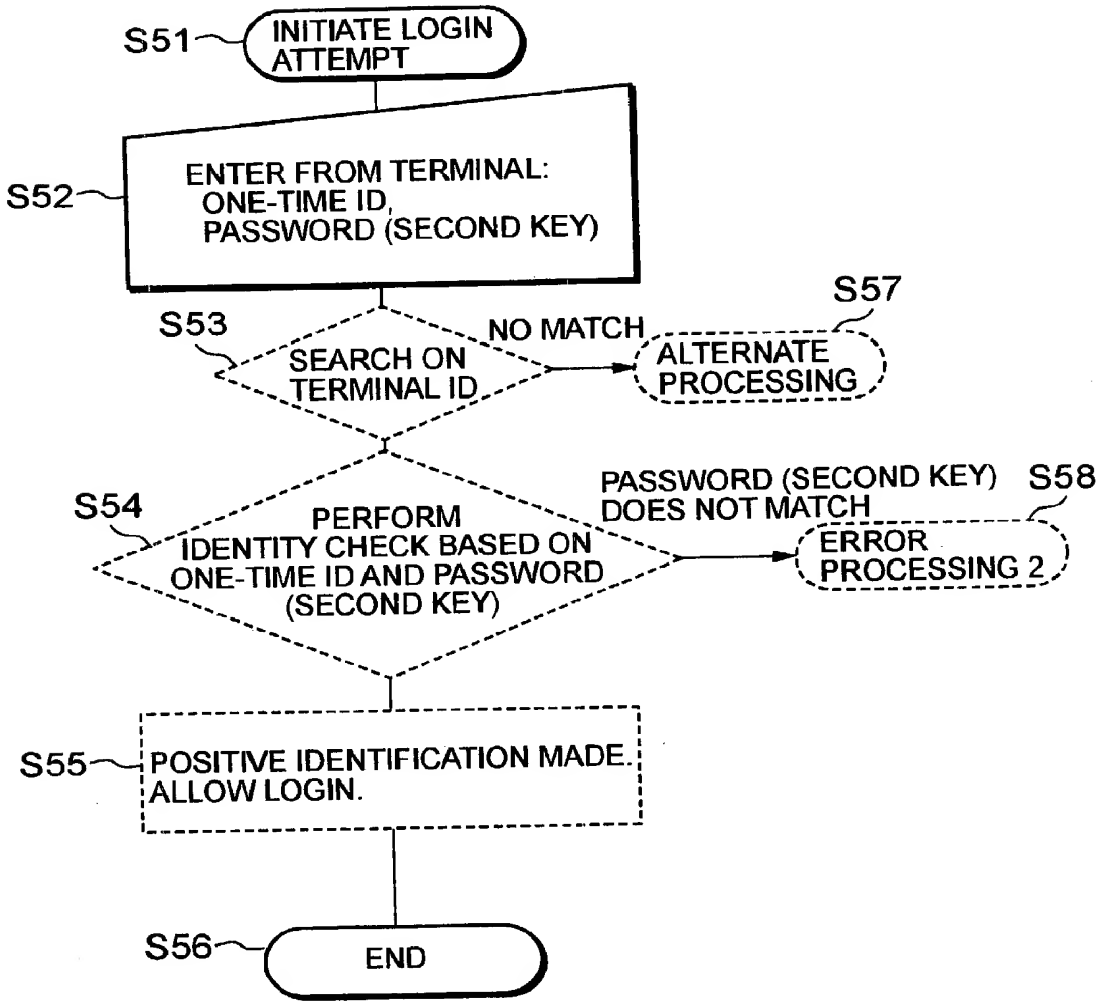

S51
INITIATE LOGIN ATTEMPT
S52
ENTER FROM TERMINAL: ONE-TIME ID, PASSWORD (SECOND KEY)
S53
SEARCH ON TERMINAL ID
NO MATCH
S57
ALTERNATE PROCESSING
S54
PERFORM IDENTITY CHECK BASED ON ONE-TIME ID AND PASSWORD (SECOND KEY)
PASSWORD (SECOND KEY) DOES NOT MATCH
S58
ERROR PROCESSING 2
S55
POSITIVE IDENTIFICATION MADE. ALLOW LOGIN.
S56
END

FIG.20

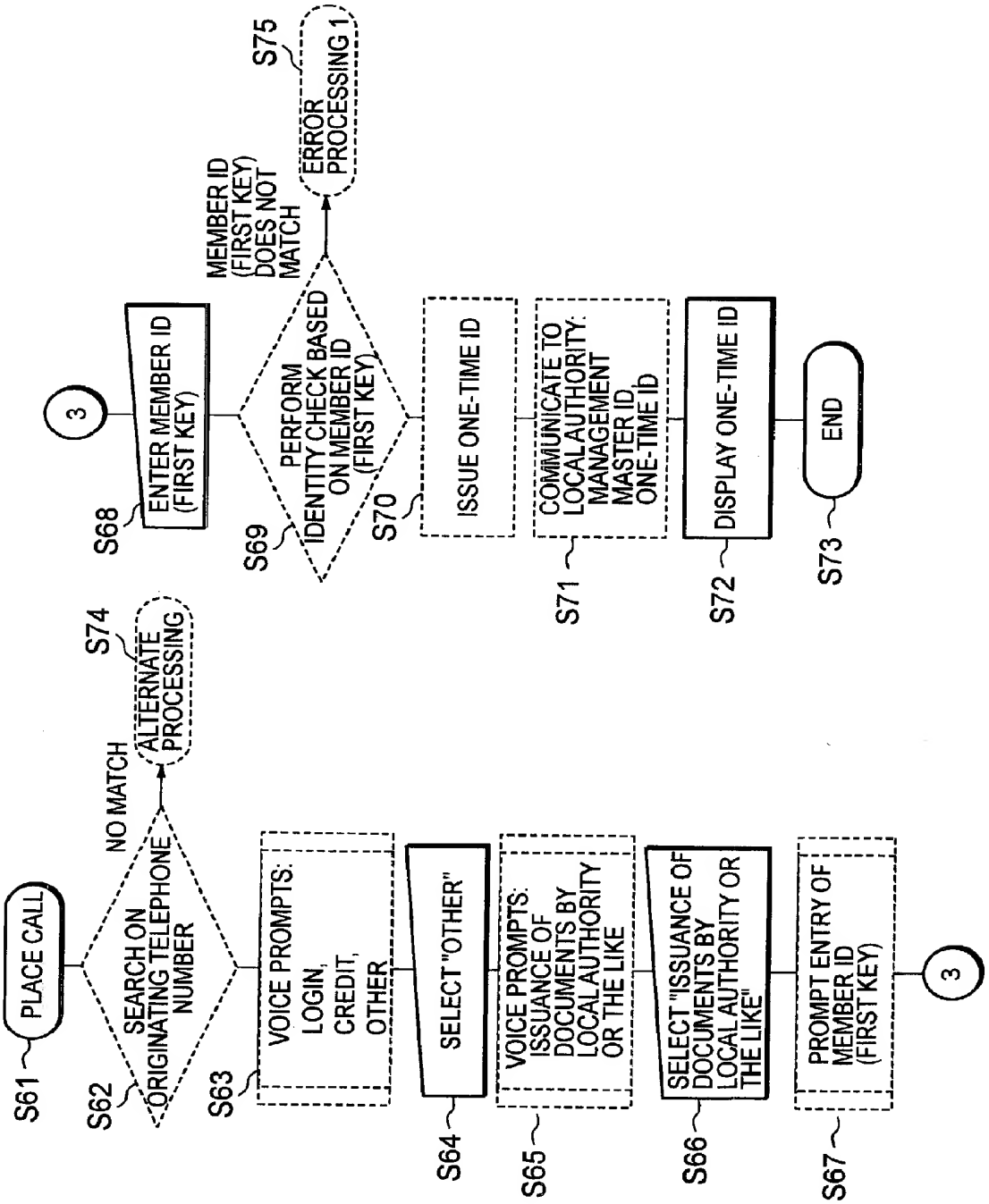

S61
PLACE CALL
S62
SEARCH ON ORIGINATING TELEPHONE NUMBER
NO MATCH
S74
ALTERNATE PROCESSING
S63
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S64
SELECT "OTHER"
S65
VOICE PROMPTS: ISSUANCE OF DOCUMENTS BY LOCAL AUTHORITY OR THE LIKE
S66
SELECT "ISSUANCE OF DOCUMENTS BY LOCAL AUTHORITY OR THE LIKE"
S67
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
3
3
S68
ENTER MEMBER ID (FIRST KEY)
S69
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
MEMBER ID (FIRST KEY) DOES NOT MATCH
S75
ERROR PROCESSING 1
S70
ISSUE ONE-TIME ID
S71
COMMUNICATE TO LOCAL AUTHORITY: MANAGEMENT MASTER ID, ONE-TIME ID
S72
DISPLAY ONE-TIME ID
S73
END

FIG. 21

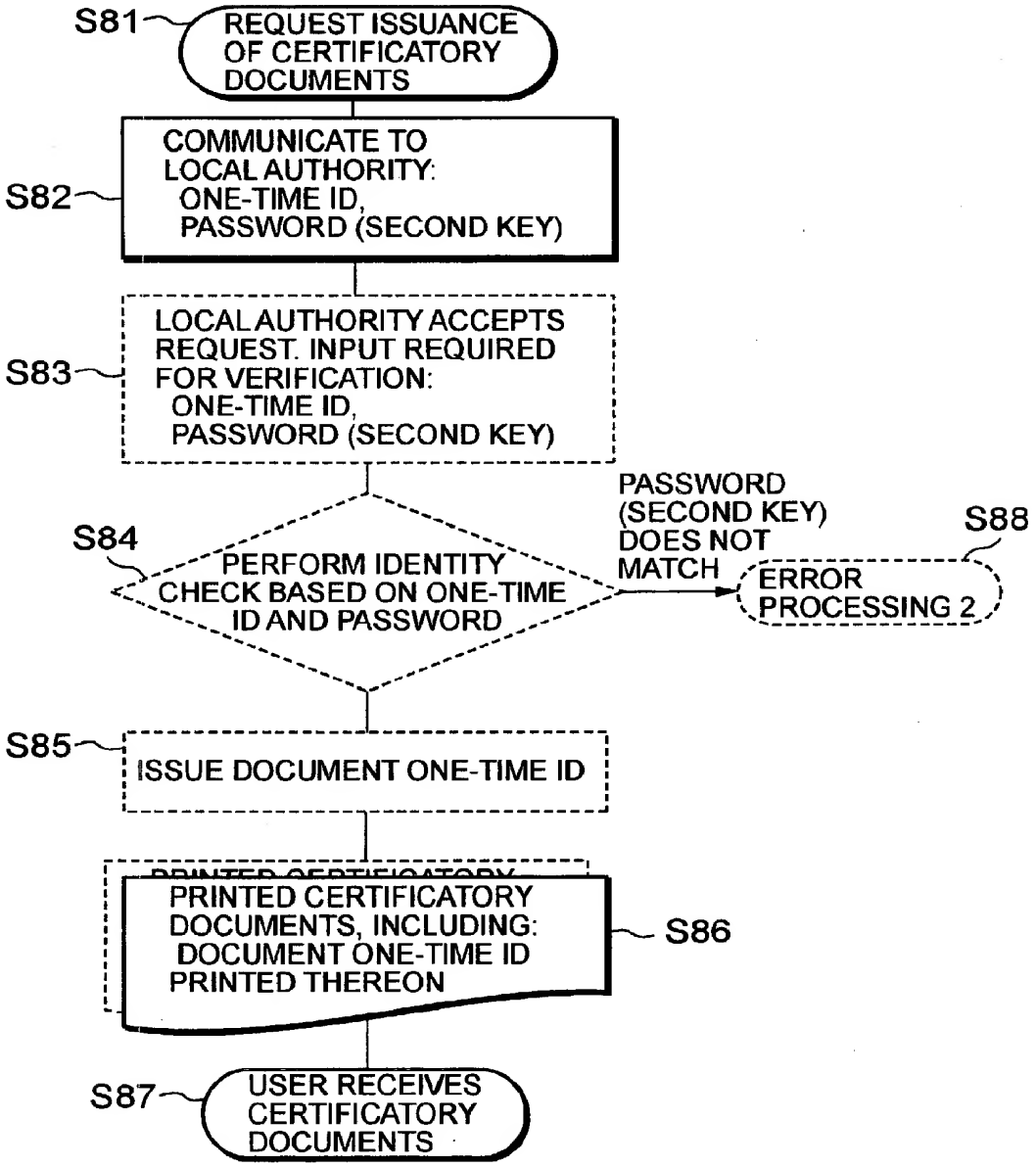

S81
REQUEST ISSUANCE OF CERTIFICATORY DOCUMENTS
COMMUNICATE TO LOCAL AUTHORITY: ONE-TIME ID, PASSWORD (SECOND KEY)
S82
LOCAL AUTHORITY ACCEPTS REQUEST. INPUT REQUIRED FOR VERIFICATION: ONE-TIME ID, PASSWORD (SECOND KEY)
S83
S84
PERFORM IDENTITY CHECK BASED ON ONE-TIME ID AND PASSWORD
PASSWORD (SECOND KEY) DOES NOT MATCH
S88
ERROR PROCESSING 2
S85
ISSUE DOCUMENT ONE-TIME ID
PRINTED CERTIFICATORY DOCUMENTS, INCLUDING: DOCUMENT ONE-TIME ID PRINTED THEREON
S86
S87
USER RECEIVES CERTIFICATORY DOCUMENTS

FIG. 22

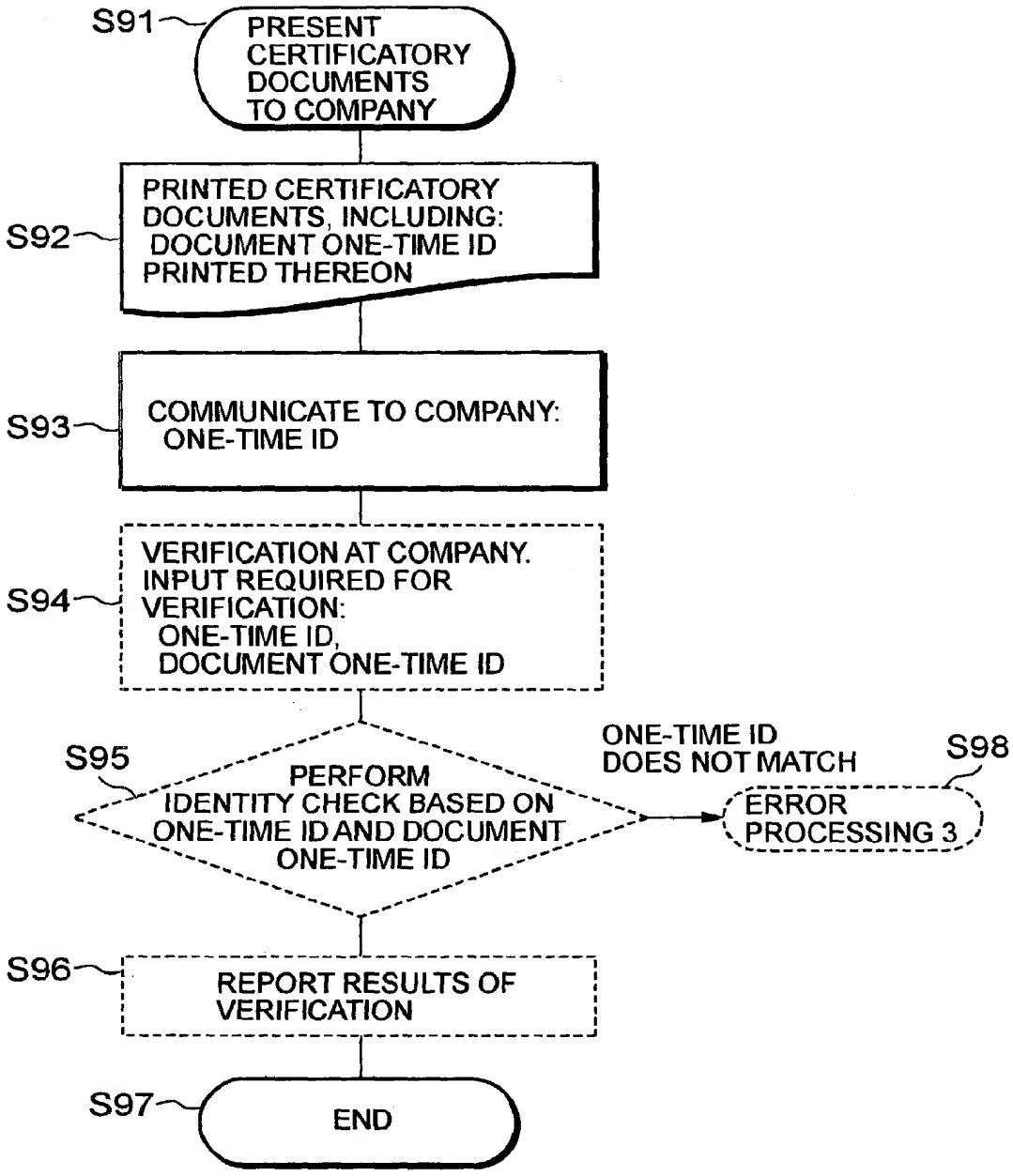

S91
PRESENT CERTIFICATORY DOCUMENTS TO COMPANY
S92
PRINTED CERTIFICATORY DOCUMENTS, INCLUDING: DOCUMENT ONE-TIME ID PRINTED THEREON
S93
COMMUNICATE TO COMPANY: ONE-TIME ID
S94
VERIFICATION AT COMPANY. INPUT REQUIRED FOR VERIFICATION: ONE-TIME ID, DOCUMENT ONE-TIME ID
S95
PERFORM IDENTITY CHECK BASED ON ONE-TIME ID AND DOCUMENT ONE-TIME ID
ONE-TIME ID DOES NOT MATCH
S98
ERROR PROCESSING 3
S96
REPORT RESULTS OF VERIFICATION
S97
END

FIG.23

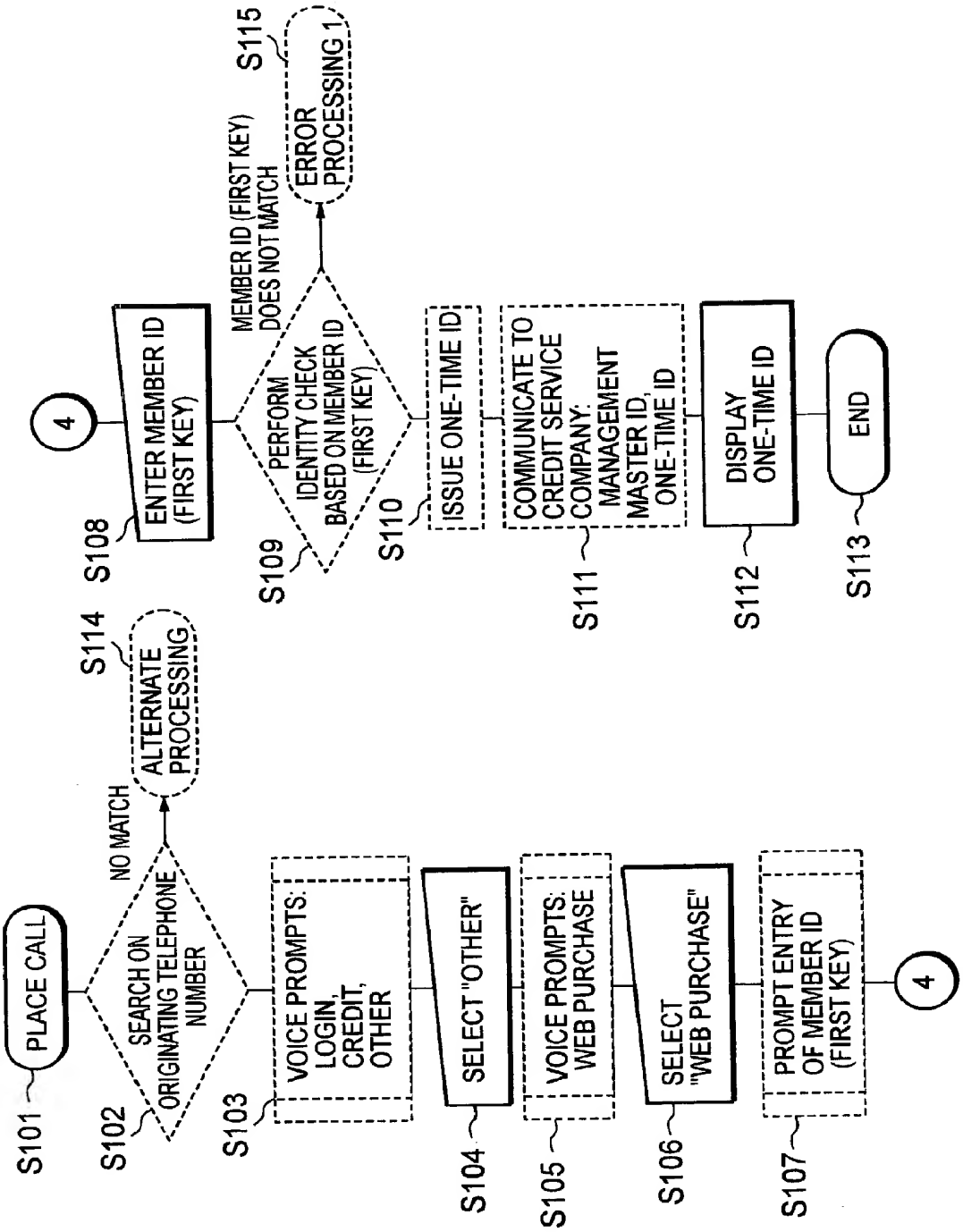

PLACE CALL
S101
SEARCH ON ORIGINATING TELEPHONE NUMBER
S102
NO MATCH
ALTERNATE PROCESSING
S114
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S103
SELECT "OTHER"
S104
VOICE PROMPTS: WEB PURCHASE
S105
SELECT "WEB PURCHASE"
S106
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S107
4
4
ENTER MEMBER ID (FIRST KEY)
S108
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S109
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1
S115
ISSUE ONE-TIME ID
S110
COMMUNICATE TO CREDIT SERVICE COMPANY: MANAGEMENT MASTER ID, ONE-TIME ID
S111
DISPLAY ONE-TIME ID
S112
END
S113

FIG.24

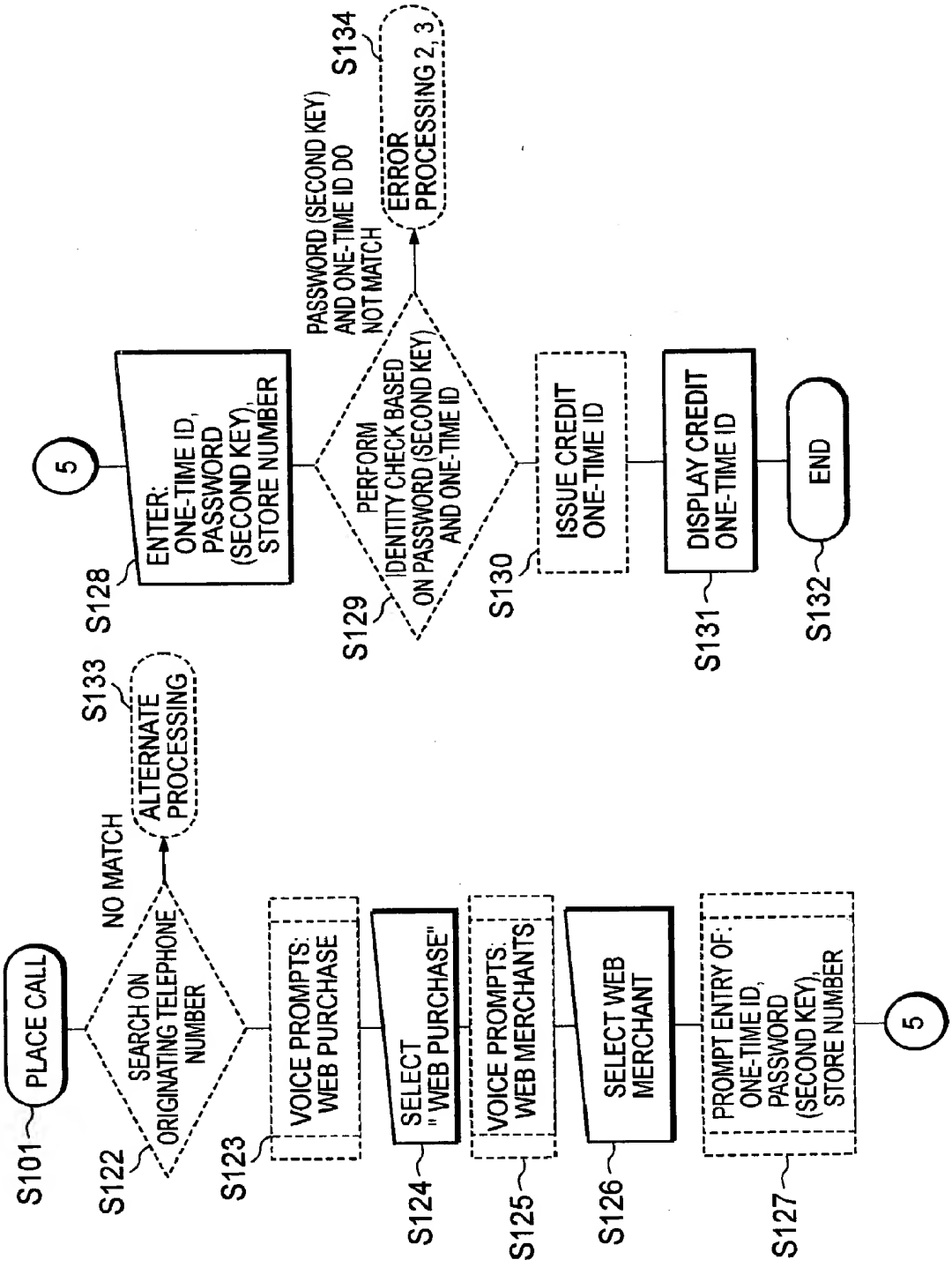

S101
PLACE CALL
S122
SEARCH ON ORIGINATING TELEPHONE NUMBER
NO MATCH
S133
ALTERNATE PROCESSING
S123
VOICE PROMPTS: WEB PURCHASE
S124
SELECT " WEB PURCHASE"
S125
VOICE PROMPTS: WEB MERCHANTS
S126
SELECT WEB MERCHANT
S127
PROMPT ENTRY OF: ONE-TIME ID, PASSWORD (SECOND KEY), STORE NUMBER
5
5
S128
ENTER: ONE-TIME ID, PASSWORD (SECOND KEY), STORE NUMBER
S129
PERFORM IDENTITY CHECK BASED ON PASSWORD (SECOND KEY) AND ONE-TIME ID
PASSWORD (SECOND KEY) AND ONE-TIME ID DO NOT MATCH
S134
ERROR PROCESSING 2, 3
S130
ISSUE CREDIT ONE-TIME ID
S131
DISPLAY CREDIT ONE-TIME ID
S132
END

FIG. 25

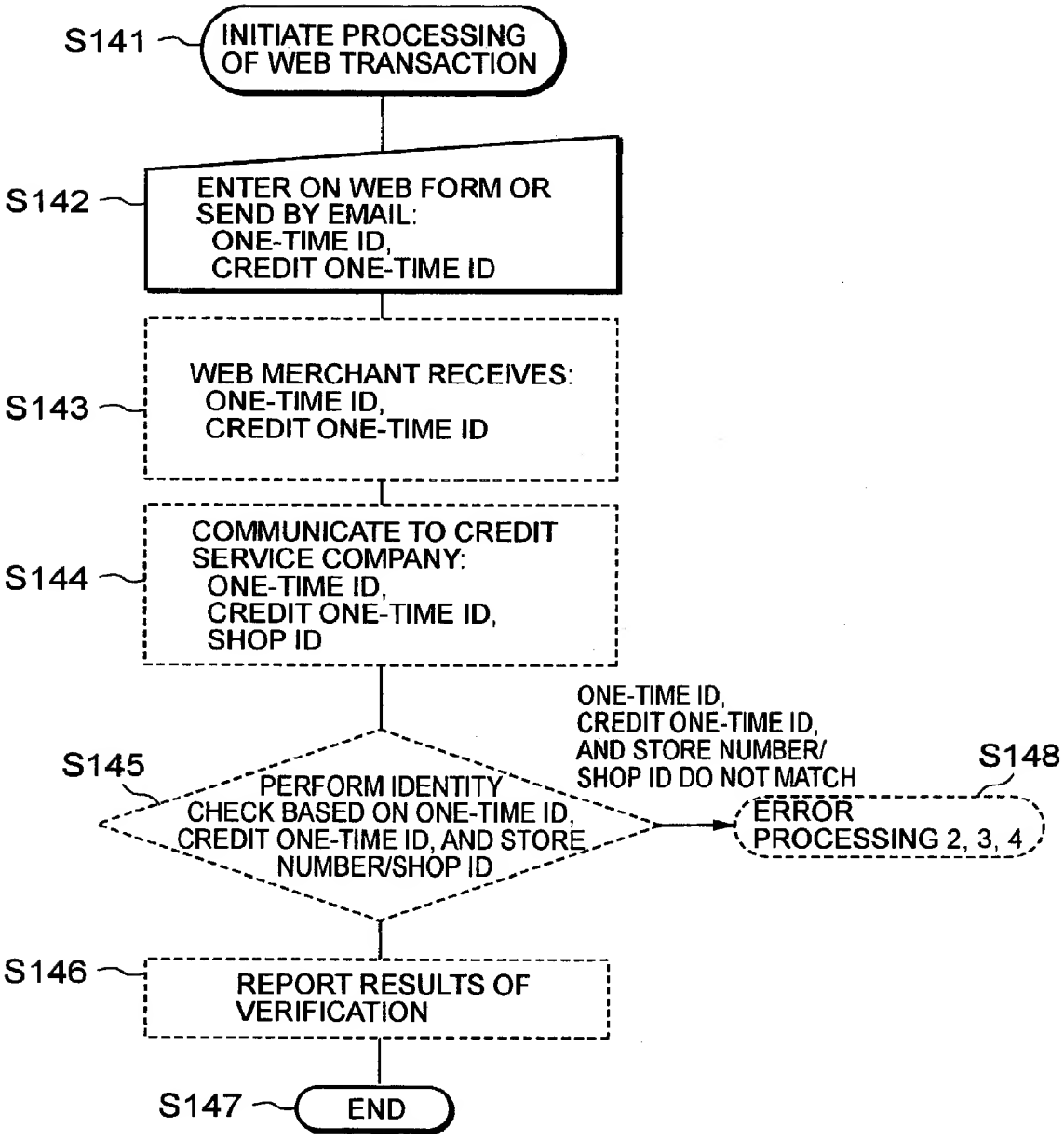

S141
INITIATE PROCESSING OF WEB TRANSACTION
S142
ENTER ON WEB FORM OR SEND BY EMAIL:
ONE-TIME ID,
CREDIT ONE-TIME ID
S143
WEB MERCHANT RECEIVES:
ONE-TIME ID,
CREDIT ONE-TIME ID
S144
COMMUNICATE TO CREDIT SERVICE COMPANY:
ONE-TIME ID,
CREDIT ONE-TIME ID,
SHOP ID
S145
PERFORM IDENTITY CHECK BASED ON ONE-TIME ID, CREDIT ONE-TIME ID, AND STORE NUMBER/SHOP ID
ONE-TIME ID, CREDIT ONE-TIME ID, AND STORE NUMBER/ SHOP ID DO NOT MATCH
S148
ERROR PROCESSING 2, 3, 4
S146
REPORT RESULTS OF VERIFICATION
S147
END

FIG.26

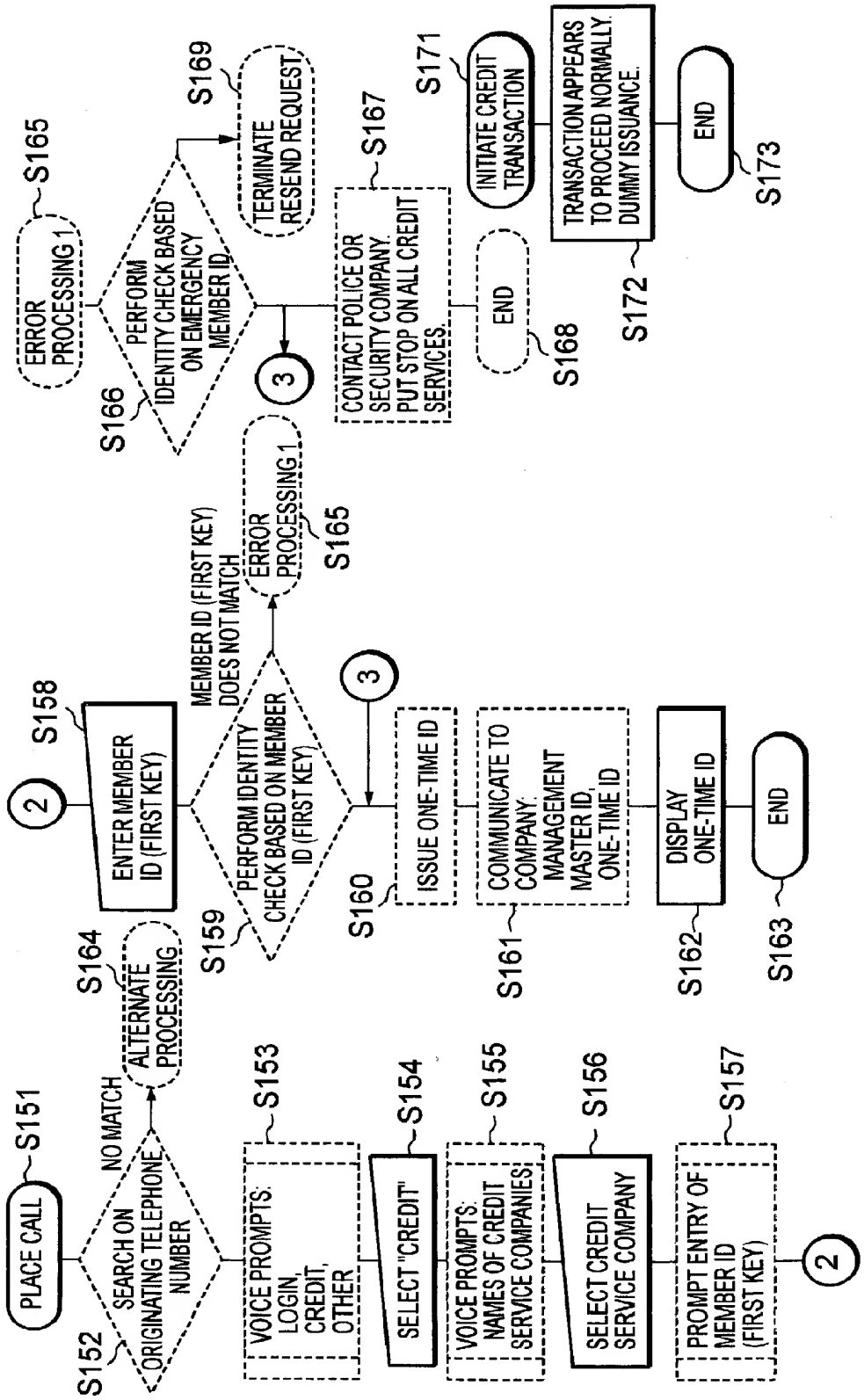

PLACE CALL
S151
SEARCH ON ORIGINATING TELEPHONE NUMBER
S152
NO MATCH
ALTERNATE PROCESSING
S164
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S153
SELECT "CREDIT"
S154
VOICE PROMPTS: NAMES OF CREDIT SERVICE COMPANIES
S155
SELECT CREDIT SERVICE COMPANY
S156
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S157
2
ENTER MEMBER ID (FIRST KEY)
S158
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S159
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1
S165
3
ISSUE ONE-TIME ID
S160
COMMUNICATE TO COMPANY: MANAGEMENT MASTER ID, ONE-TIME ID
S161
DISPLAY ONE-TIME ID
S162
END
S163
ERROR PROCESSING 1
S165
PERFORM IDENTITY CHECK BASED ON EMERGENCY MEMBER ID
S166
TERMINATE RESEND REQUEST
S169
3
CONTACT POLICE OR SECURITY COMPANY. PUT STOP ON ALL CREDIT SERVICES.
S167
END
S168
INITIATE CREDIT TRANSACTION
S171
TRANSACTION APPEARS TO PROCEED NORMALLY. DUMMY ISSUANCE.
S172
END
S173

FIG.27

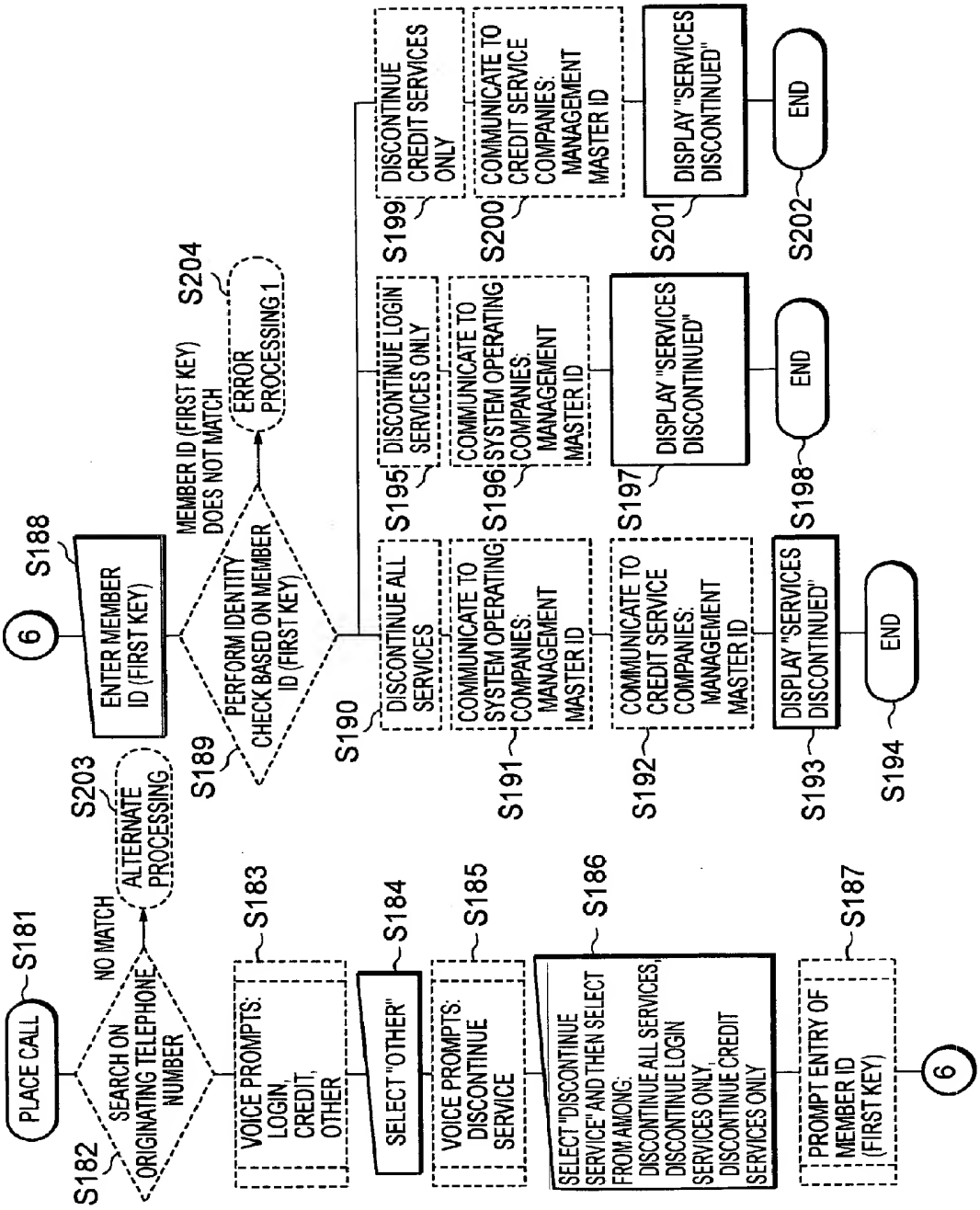

PLACE CALL
S181
SEARCH ON ORIGINATING TELEPHONE NUMBER
S182
NO MATCH
ALTERNATE PROCESSING
S203
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S183
SELECT "OTHER"
S184
VOICE PROMPTS: DISCONTINUE SERVICE
S185
SELECT "DISCONTINUE SERVICE" AND THEN SELECT FROM AMONG: DISCONTINUE ALL SERVICES, DISCONTINUE LOGIN SERVICES ONLY, DISCONTINUE CREDIT SERVICES ONLY
S186
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S187
6
6
ENTER MEMBER ID (FIRST KEY)
S188
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S189
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1
S204
DISCONTINUE ALL SERVICES
S190
COMMUNICATE TO SYSTEM OPERATING COMPANIES: MANAGEMENT MASTER ID
S191
COMMUNICATE TO CREDIT SERVICE COMPANIES: MANAGEMENT MASTER ID
S192
DISPLAY "SERVICES DISCONTINUED"
S193
END
S194
DISCONTINUE LOGIN SERVICES ONLY
S195
COMMUNICATE TO SYSTEM OPERATING COMPANIES: MANAGEMENT MASTER ID
S196
DISPLAY "SERVICES DISCONTINUED"
S197
END
S198
DISCONTINUE CREDIT SERVICES ONLY
S199
COMMUNICATE TO CREDIT SERVICE COMPANIES: MANAGEMENT MASTER ID
S200
DISPLAY "SERVICES DISCONTINUED"
S201
END
S202

FIG.28

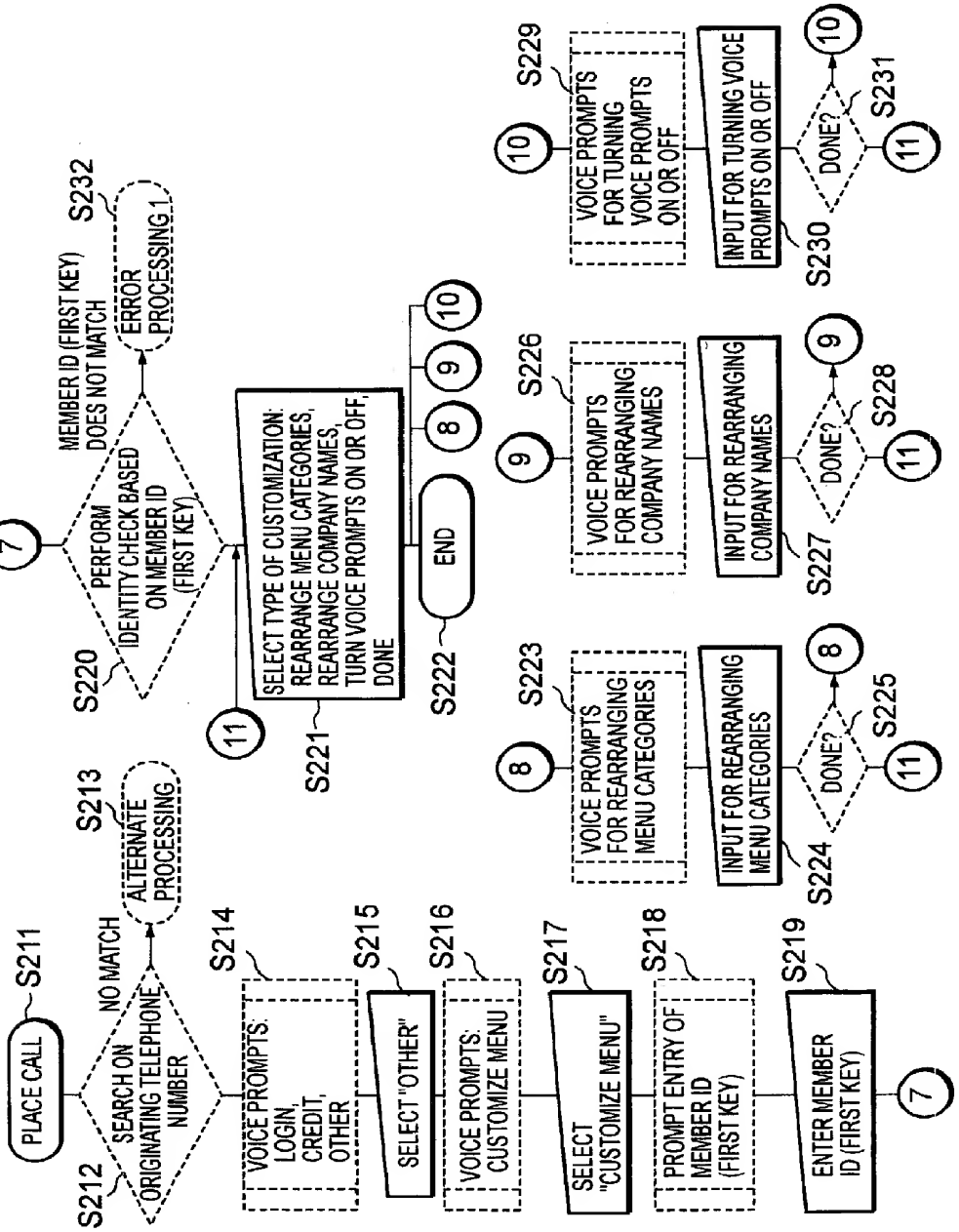
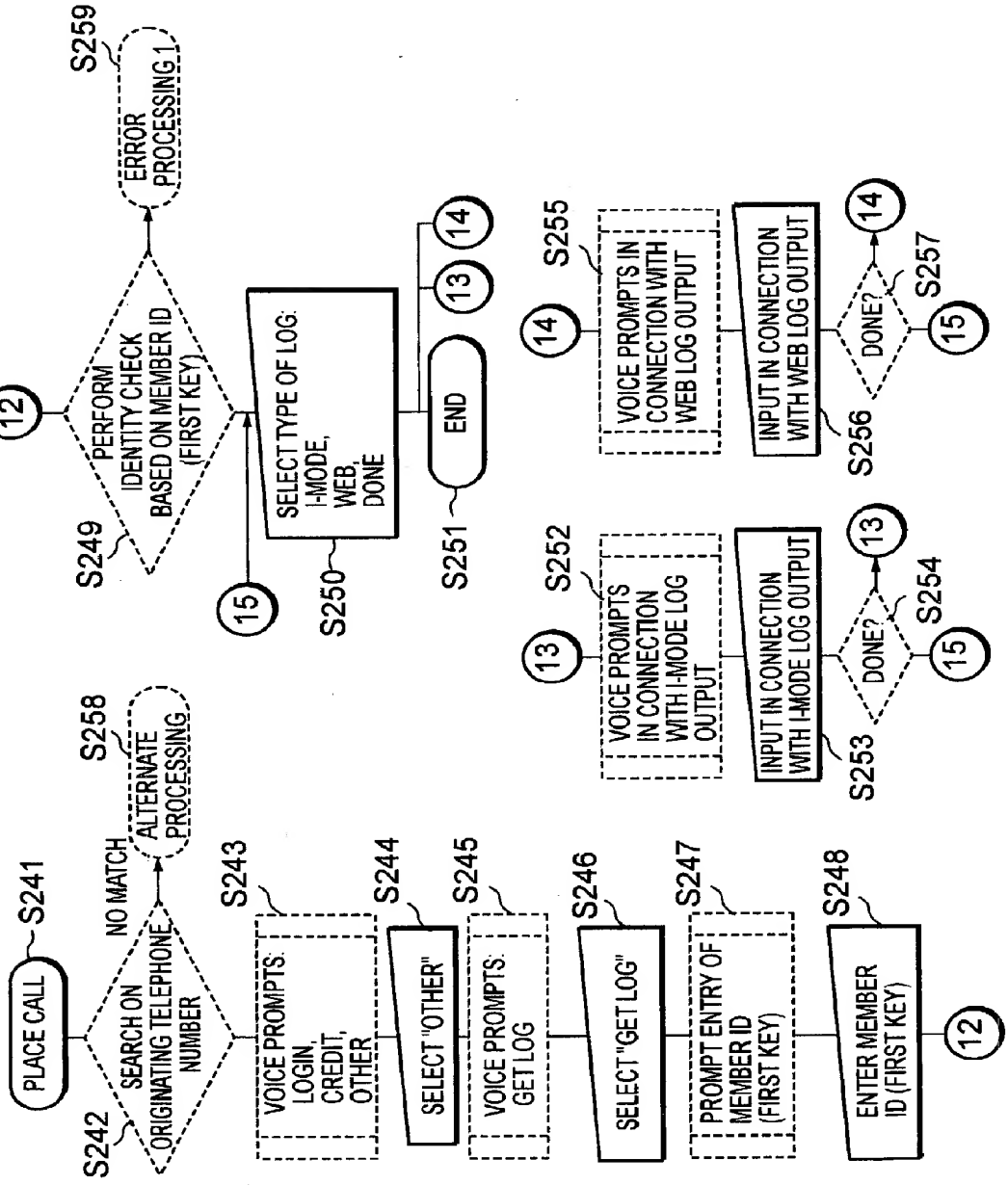

PLACE CALL
S211
SEARCH ON ORIGINATING TELEPHONE NUMBER
S212
NO MATCH
ALTERNATE PROCESSING
S213
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S214
SELECT "OTHER"
S215
VOICE PROMPTS: CUSTOMIZE MENU
S216
SELECT "CUSTOMIZE MENU"
S217
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S218
ENTER MEMBER ID (FIRST KEY)
S219
7
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S220
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1
S232
11
SELECT TYPE OF CUSTOMIZATION: REARRANGE MENU CATEGORIES, REARRANGE COMPANY NAMES, TURN VOICE PROMPTS ON OR OFF, DONE
S221
END
S222
8
VOICE PROMPTS FOR REARRANGING MENU CATEGORIES
S223
INPUT FOR REARRANGING MENU CATEGORIES
DONE?
S224
S225
9
VOICE PROMPTS FOR REARRANGING COMPANY NAMES
S226
INPUT FOR REARRANGING COMPANY NAMES
DONE?
S227
S228
10
VOICE PROMPTS FOR TURNING VOICE PROMPTS ON OR OFF
S229
INPUT FOR TURNING VOICE PROMPTS ON OR OFF
DONE?
S230
S231

FIG.29


PLACE CALL
S241
SEARCH ON ORIGINATING TELEPHONE NUMBER
S242
NO MATCH
ALTERNATE PROCESSING
S258
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S243
SELECT "OTHER"
S244
VOICE PROMPTS: GET LOG
S245
SELECT "GET LOG"
S246
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S247
ENTER MEMBER ID (FIRST KEY)
S248
12
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S249
ERROR PROCESSING 1
S259
15
SELECT TYPE OF LOG: I-MODE, WEB, DONE
S250
END
S251
13
14
VOICE PROMPTS IN CONNECTION WITH I-MODE LOG OUTPUT
S252
INPUT IN CONNECTION WITH I-MODE LOG OUTPUT
S253
DONE?
S254
VOICE PROMPTS IN CONNECTION WITH WEB LOG OUTPUT
S255
INPUT IN CONNECTION WITH WEB LOG OUTPUT
S256
DONE?
S257

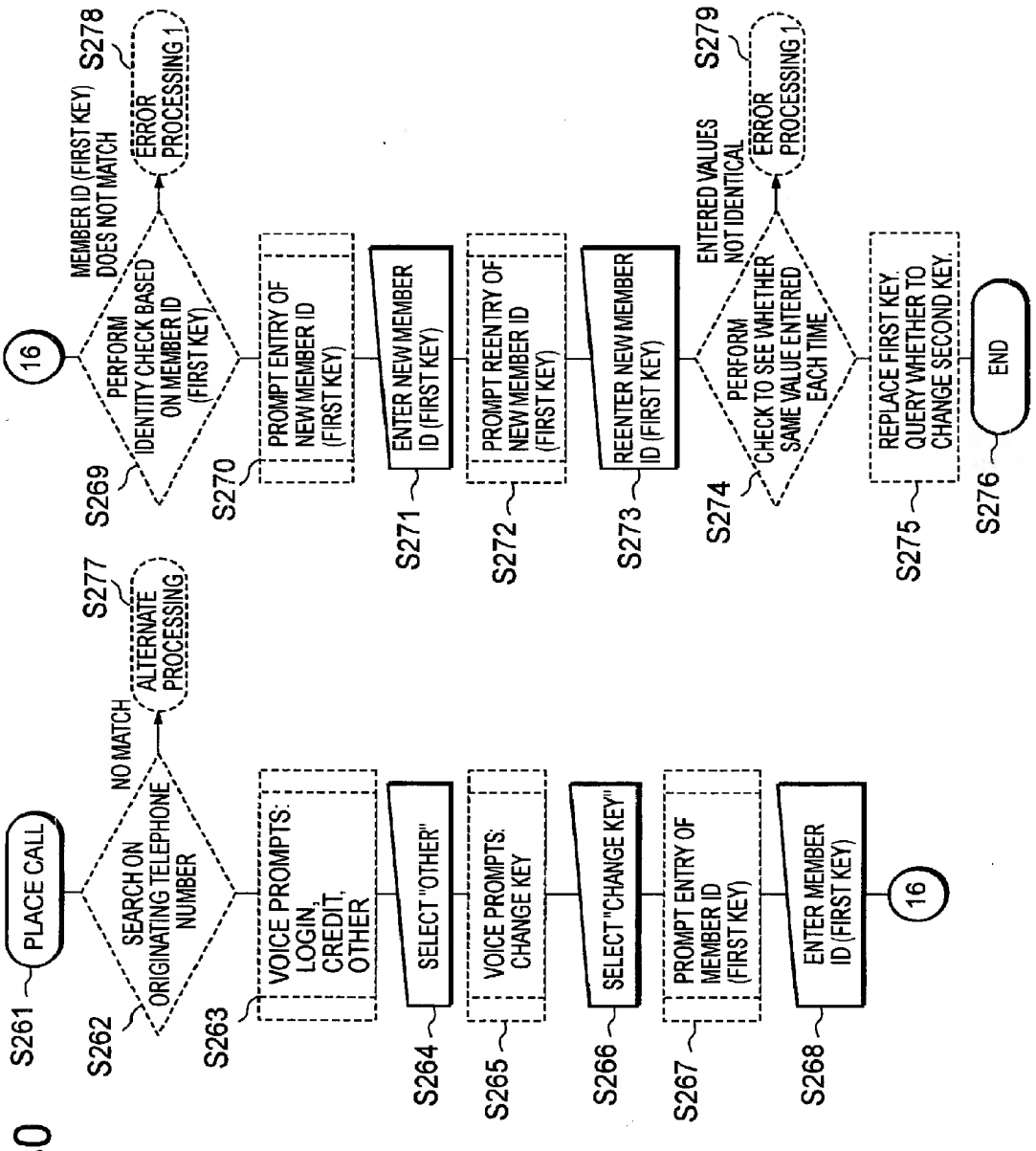

PLACE CALL
S261
SEARCH ON ORIGINATING TELEPHONE NUMBER
S262
NO MATCH
ALTERNATE PROCESSING
S277
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S263
SELECT "OTHER"
S264
VOICE PROMPTS: CHANGE KEY
S265
SELECT "CHANGE KEY"
S266
PROMPT ENTRY OF MEMBER ID (FIRST KEY)
S267
ENTER MEMBER ID (FIRST KEY)
S268
16
16
PERFORM IDENTITY CHECK BASED ON MEMBER ID (FIRST KEY)
S269
MEMBER ID (FIRST KEY) DOES NOT MATCH
ERROR PROCESSING 1.
S278
PROMPT ENTRY OF NEW MEMBER ID (FIRST KEY)
S270
ENTER NEW MEMBER ID (FIRST KEY)
S271
PROMPT REENTRY OF NEW MEMBER ID (FIRST KEY)
S272
REENTER NEW MEMBER ID (FIRST KEY)
S273
PERFORM CHECK TO SEE WHETHER SAME VALUE ENTERED EACH TIME
S274
ENTERED VALUES NOT IDENTICAL
ERROR PROCESSING 1.
S279
REPLACE FIRST KEY. QUERY WHETHER TO CHANGE SECOND KEY.
S275
END
S276

FIG.30

FIG.31

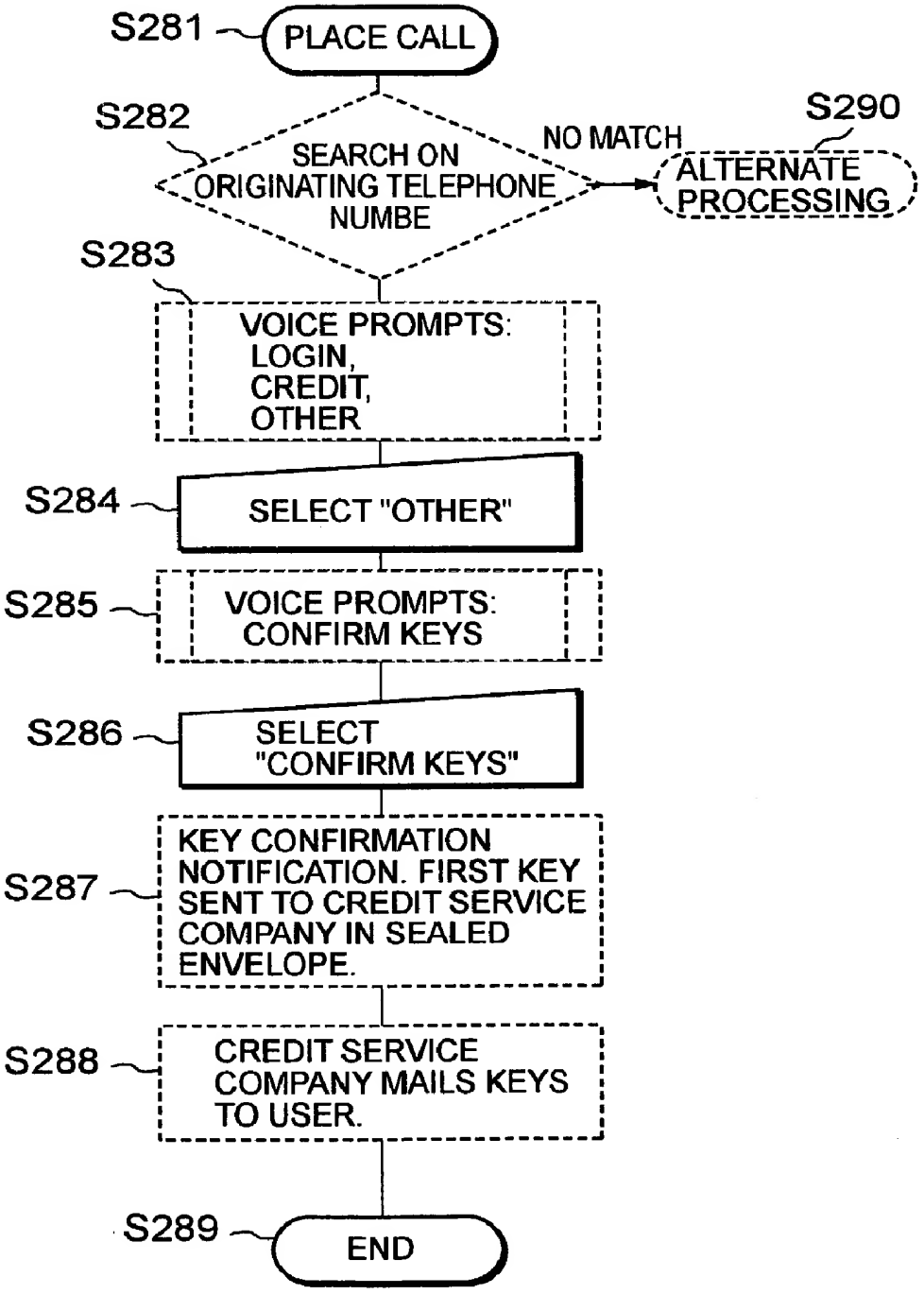
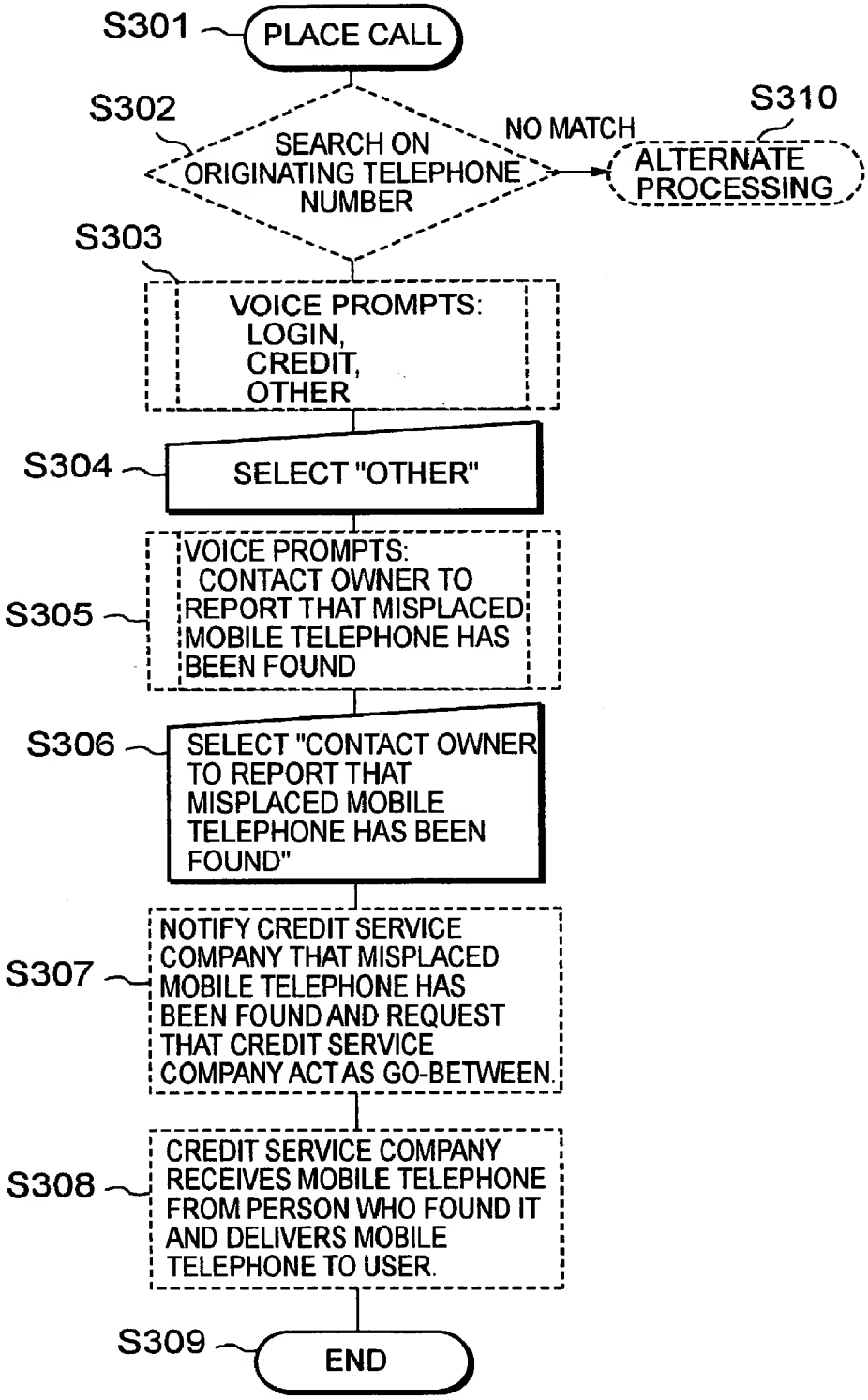

S281
PLACE CALL
S282
SEARCH ON ORIGINATING TELEPHONE NUMBE
NO MATCH
S290
ALTERNATE PROCESSING
S283
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S284
SELECT "OTHER"
S285
VOICE PROMPTS: CONFIRM KEYS
S286
SELECT "CONFIRM KEYS"
S287
KEY CONFIRMATION NOTIFICATION. FIRST KEY SENT TO CREDIT SERVICE COMPANY IN SEALED ENVELOPE.
S288
CREDIT SERVICE COMPANY MAILS KEYS TO USER.
S289
END

FIG.32


S301
PLACE CALL
S302
SEARCH ON ORIGINATING TELEPHONE NUMBER
NO MATCH
S310
ALTERNATE PROCESSING
S303
VOICE PROMPTS: LOGIN, CREDIT, OTHER
S304
SELECT "OTHER"
S305
VOICE PROMPTS: CONTACT OWNER TO REPORT THAT MISPLACED MOBILE TELEPHONE HAS BEEN FOUND
S306
SELECT "CONTACT OWNER TO REPORT THAT MISPLACED MOBILE TELEPHONE HAS BEEN FOUND"
S307
NOTIFY CREDIT SERVICE COMPANY THAT MISPLACED MOBILE TELEPHONE HAS BEEN FOUND AND REQUEST THAT CREDIT SERVICE COMPANY ACT AS GO-BETWEEN.
S308
CREDIT SERVICE COMPANY RECEIVES MOBILE TELEPHONE FROM PERSON WHO FOUND IT AND DELIVERS MOBILE TELEPHONE TO USER.
S309
END

METHOD AND SYSTEM FOR VERIFYING IDENTITY

BACKGROUND

[0001] The present invention pertains to a method and system for electronically ascertaining whether a person attempting some action, e.g., someone attempting to process a credit card transaction or to log on to a server or the like, is in fact a person authorized to perform such action.

[0002] Systems for verifying personal identity through use of an IC card, smart card, or the like in the possession of such person are known in the art. Furthermore, systems for verifying personal identity through use of an ID (e.g., telephone number) of a mobile telephone in the possession of such person are known in the art. However, such systems, rather than ascertaining the identity of the person in question, substitute ascertainment of the fact of use of such equipment (serving as a tool for such purpose) for verification of personal identity. A third party using such equipment and pretending to be the person in question might easily outwit such a system.

[0003] Also known in the art are systems for verifying personal identity whereby a user ID-password set unique to a person is input into the system by the person in question, and authentication is carried out using that user ID-password set. However, by intercepting communication between that person and the system, a third party might gain access to the user ID-password set and might make illicit use of same.

[0004] To improve reliability of authentication, systems for verifying personal identity making use of temporary or one-time IDs good for only a single use are known in the art. The systems described at Japanese Patent Application Publication Kokai No. H12-10927 (2000), Japanese Patent Application Publication Kokai No. H13-175599 (2001), Japanese Patent Application Publication Kokai No. H14-7355 (2002) and the like may be cited as examples. However, in all of these systems, for a one-time ID to be issued, a set comprising an ID of a mobile telephone or a user ID and a password must be input into the system, just as was the case with the other conventional systems described above. This being the case, here again a third party might use the mobile telephone and pretend to be the person in question, or might intercept communication to gain access to the user ID-password set, allowing the third party to acquire a one-time ID in the same fashion as the person in question, which might then be used for some illicit purpose by the third party.

[0005] Moreover, as more reliable systems for verifying personal identity, arrangements making use of biometric equipment are known and have recently even become something of a fad. However, the fact that expensive biometric equipment must be purchased makes this an unattractive option for use in verifying personal identity for the everyday sorts of actions performed by large numbers of people, such as those involving processing of credit transactions or logging on to a system.

SUMMARY

[0006] It is an object of the present invention to provide a mechanism by which personal identity may be verified that is inexpensive and yet reliable.

[0007] In a method for verifying identity in accordance with a first aspect of the present invention, only first key or keys of one or more users possessing both first key or keys and second key or keys is or are saved by one or more first systems, and only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved by one or more second systems. First key(s) and second key(s) may thus be separately saved by different systems or groups of systems. The different systems or groups of systems may keep their respective keys secret from each other.

[0008] At least one of the first system or systems may receive input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and may carry out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users. If at least one positive verification of identity is made at at least one of the first-stage identity check or checks, at least one of the first system or systems may cause one or more one-time IDs to be issued to at least one of the user or users. At least one of the first system or systems may communicate to at least one of the second system or systems at least one of the one-time ID or IDs issued to at least one of the user or users. At least one of the second system or systems may save at least one of the one-time ID or IDs communicated thereto by the at least one first system.

[0009] At least one of the second system or systems may receive input of data purporting to be at least one of the second key or keys and at least one of the one-time ID or IDs and may carry out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved one-time ID or IDs of at least one of the user or users. Provision of one or more services to at least one of the user or users may be controlled in correspondence to at least one result of at least one of the second-stage identity check or checks.

[0010] In a preferred embodiment, at least one of the first system or systems may, in addition to the first key or keys, also save one or more identification numbers of one or more mobile communication terminals of at least one of the user or users. Furthermore, in such a preferred embodiment, at least one of the first system or systems may receive input of data purporting to be at least one of the first key or keys by way of one or more mobile communication terminals from at least one of the party or parties purporting to be at least one of the user or users, and may carry out at least one of the first-stage identity check or checks by comparing at least one of the input purported first key or keys and at least one identification number of at least one of the mobile communication terminal or terminals used for input thereof to at least one of the saved first key or keys and at least one of the saved identification number or numbers of at least one of the mobile communication terminal or terminals of at least one of the user or users.

[0011] In a preferred embodiment, at least one of the first system or systems may further save one or more facial images of at least one of the user or users. Furthermore, in such a preferred embodiment, if at least one positive veri-

fication of identity is made at at least one of the first-stage identity check or checks, at least one of the first system or systems may, in addition to the one or more one-time IDs, cause at least one of the saved facial image or images of at least one of the user or users to be issued to at least one of the user or users in such fashion as to permit display thereof by at least one of the user or users.

[0012] In a method for verifying identity in accordance with another aspect of the present invention, first key or keys and second key or keys of user or users may be saved in mutually secret fashion to separate first system or systems and second system or systems as described above. Furthermore, at least one of the first system or systems may receive input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and may carry out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users. If at least one positive verification of identity is made at at least one of the first-stage identity check or checks, at least one of the first system or systems may cause one or more first one-time IDs to be issued to at least one of the user or users, and may communicate to at least one of the second system or systems at least one of the first one-time ID or IDs issued to at least one of the user or users. At least one of the second system or systems may save at least one of the first one-time ID or IDs communicated thereto by the at least one first system.

[0013] At least one of the second system or systems may thereafter receive input of data purporting to be at least one of the second key or keys and at least one of the first one-time ID or IDs from one or more parties purporting to be at least one of the user or users and may carry out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported first one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved first one-time ID or IDs of at least one of the user or users. If at least one positive verification of identity is made at at least one of the second-stage identity check or checks, at least one of the second system or systems may cause one or more second one-time IDs to be issued to at least one of the user or users and may save at least one of the issued second one-time ID or IDs.

[0014] At least one of the second system or systems may receive input of data purporting to be at least one of the first one-time ID or IDs and at least one of the second one-time ID or IDs, and may carry out one or more third-stage identity checks by comparing at least one of the input purported first one-time ID or IDs and at least one of the input purported second one-time ID or IDs to at least one of the saved first one-time ID or IDs and at least one of the saved second one-time ID or IDs of at least one of the user or users. Provision of one or more services to at least one of the user or users may be controlled in correspondence to at least one result of at least one of the third-stage identity check or checks.

BRIEF DESCRIPTION OF DRAWINGS

[0015] These and other features, aspects, and advantages of the present invention will become better understood with reference to the following description, appended claims, and accompanying drawings where:

[0016] **FIG. 1** is a block diagram showing basic constitution and operation in one embodiment of a method for verifying identity in accordance with the present invention;

[0017] **FIG. 2** is a block diagram showing a method for registering keys and so forth which may be employed in this embodiment;

[0018] **FIG. 3** is a block diagram showing an application in the context of verification of identity such as might be carried out during processing of credit transaction(s);

[0019] **FIG. 4** is a block diagram showing an application in the context of verification of identity such as might be carried out when logging on to server(s);

[0020] **FIG. 5** is a block diagram showing an application in the context of verification of identity such as might be carried out when certificatory document(s) issued by a local authority or the like is or are to be presented to user(s) **1**;

[0021] **FIG. 6** is a block diagram showing an application in the context of verification of identity such as might be carried out during processing of credit transaction(s) when making purchase(s) over the Internet from web merchant(s);

[0022] **FIG. 7** is a block diagram showing a variation in which encryption processing is added to the application in the context of logging on to server(s) shown in **FIG. 4**;

[0023] **FIG. 8** is a block diagram showing a variation in which facial composite processing is added to the application in the context of credit transaction processing shown in **FIG. 3**;

[0024] **FIG. 9** is a block diagram showing a situation where a third party acquires a mobile telephone belonging to a user and uses same to pretend to be that user;

[0025] **FIG. 10** is a block diagram showing a situation where a store attempts to defraud a credit service company;

[0026] **FIG. 11** is a block diagram showing a situation where a third party gains possession of data through electronic interception thereof;

[0027] **FIG. 12** is a block diagram showing another situation where a third party gains possession of data through electronic interception thereof;

[0028] **FIG. 13** is a block diagram showing constitution of a database **4** that might be associated with verification facilitating system(s) **3**;

[0029] **FIG. 14** is a block diagram showing constitution of a database **7** that might be associated with verifying system(s) **6**;

[0030] **FIG. 15** is a drawing showing an example of a service menu that might be provided to mobile telephone(s) **2** of user(s) **1** by verification facilitating system(s) **3**;

[0031] **FIG. 16** is a flowchart showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** in the context of an exemplary application involving processing of credit transaction(s) as shown in **FIG. 3**;

[0032] **FIG. 17** is a flowchart showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) **6** in the

context of an exemplary application involving processing of credit transaction(s) as shown in **FIG. 3**;

[**0033**] **FIG. 18** is a flowchart showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** in the context of an exemplary application involving logging on to server(s) as shown in **FIG. 4**;

[**0034**] **FIG. 19** is a flowchart showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) (server(s)) **6** in the context of an exemplary application involving logging on to server(s) as shown in **FIG. 4**;

[**0035**] **FIG. 20** is a flowchart showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** in the context of an exemplary application involving issuance of certificatory document(s) by a local authority or the like as shown in **FIG. 5**;

[**0036**] **FIG. 21** is a flowchart showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) (document issuing system(s)) **6** in the context of an exemplary application involving issuance of certificatory document(s) by a local authority or the like as shown in **FIG. 5**;

[**0037**] **FIG. 22** is a flowchart showing a sequence of operations in connection with third-stage identity check(s) that might be carried out by verifying system(s) (document issuing system(s)) **6** in the context of an exemplary application involving issuance of certificatory document(s) by a local authority or the like as shown in **FIG. 5**;

[**0038**] **FIG. 23** is a flowchart showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** in the context of an exemplary application involving processing of credit transaction(s) when making purchase(s) during web shopping as shown in **FIG. 6**;

[**0039**] **FIG. 24** is a flowchart showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) **6** of credit service company or companies in the context of an exemplary application involving processing of credit transaction(s) when making purchase(s) during web shopping as shown in **FIG. 6**;

[**0040**] **FIG. 25** is a flowchart showing a sequence of operations in connection with third-stage identity check(s) that might be carried out by verifying system(s) **6** of credit service company or companies in the context of an exemplary application involving processing of credit transaction(s) when making purchase(s) during web shopping as shown in **FIG. 6**;

[**0041**] **FIG. 26** is a flowchart showing a sequence of operations that might occur during emergency communication using an emergency member ID and dummy verification processing;

[**0042**] **FIG. 27** is a flowchart showing a sequence of operations for discontinuing a service;

[**0043**] **FIG. 28** is a flowchart showing a sequence of operations in connection with menu customization functionality;

[**0044**] **FIG. 29** is a flowchart showing a sequence of operations in connection with functionality for retrieving and displaying a log of accessed websites;

[**0045**] **FIG. 30** is a flowchart showing a sequence of operations for changing key(s);

[**0046**] **FIG. 31** is a flowchart showing a sequence of operations for receiving confirmation of key content; and

[**0047**] **FIG. 32** is a flowchart showing a sequence of operations for contacting the owner of a misplaced mobile telephone which is found by a third party.

DESCRIPTION

[**0048**] Below, several exemplary embodiments of the present invention are described in detail with reference to the drawings

[**0049**] **FIG. 1** shows basic constitution and operation in one embodiment of a method for verifying identity in accordance with the present invention. Note that as used herein, the terms "verification,""identification,""authentication," and the like are used essentially interchangeably, without intention to limit the invention thereby.

[**0050**] Referring to the lower half of **FIG. 1**, when certain user(s) **1** attempts or attempt to use particular service(s) provided by particular organization(s) Y (e.g., when attempting to use credit transaction processing service(s) of particular credit service company or companies, when attempting to log on to server(s) of company or companies operating particular system(s), or the like), organization(s) Y may carry out identity check(s) to ascertain that user(s) **1** is or are in fact among one or more previously registered person(s) entitled to receive that particular service or those particular services. Organization(s) Y thus having need to verify identity of user(s) **1** will be referred to as "verifying company" in the present specification, the singular being used for the sake of brevity but without intention to exclude the possibility of a plurality thereof. To carry out identity check or checks on user(s) **1** (and optionally to in addition carry out processing in connection with such particular service(s)), verifying company Y may have computer system(s) (hereinafter "verifying system(s)") **6**. Such verifying system(s) **6** may be capable of communication with terminal(s) **5**, any number of which may be utilized directly or indirectly when user(s) **1** attempts or attempt to receive the particular service(s). For example, if user(s) **1** attempts or attempt to purchase goods involving processing of credit transaction(s) by certain store(s), such terminal(s) **5** might correspond to point-of-sale ("POS") terminal(s) at the store(s); if user(s) **1** attempts or attempt to log on to certain server(s) from personal computer(s) belonging to user(s) **1**, such terminal(s) **5** might correspond to that or those personal computer(s); and so forth.

[**0051**] Furthermore, referring to the top half of **FIG. 1**, organization(s) X for facilitating such processing for verification of identity carried out by verifying company Y may be provided separately from verifying company Y. Organization(s) X for facilitating such verification will be referred to as "verification facilitating company" in the present specification, the singular being used for the sake of brevity but without intention to exclude the possibility of a plurality thereof To carry out processing for facilitating such verification, verification facilitating company X may have com-

puter system(s) (hereinafter "verification facilitating system(s)") **3**. Verification facilitating system(s) **3** may moreover be capable of communication with verifying system(s) **6**.

[0052] User(s) **1** may possess mobile communication terminal(s) **2**. In the present embodiment, mobile communication terminal(s) **2** of user(s) **1** may be mobile telephone(s) (but note that mobile telephone(s) are here cited only by way of example, it being possible to alternatively or additionally use other types of mobile communication terminals such as, for example, PDAs, laptop- or notebook-type personal computers, car navigation apparatuses, and so forth). Mobile telephone(s) **2** of user(s) **1** may be capable of communication with verification facilitating system(s) **3**.

[0053] User(s) **1** may have two keys or sets of keys, i.e., first key(s) and second key(s), these being unique to such user(s) **1**. In the description that follows, whereas such first such key(s) will be referred to as "member ID(s)" and such second key(s) will be referred to as "password(s)," this is merely for the sake of convenience in distinguishing between such keys or sets of keys and is not intended to limit the scope of the invention, the important thing from the standpoint of the invention being not the particular word which is used but the whether the role of the corresponding element(s) in the present invention is served. User(s) **1** preferably keep such "member ID(s)" and "password(s)," these being unique to such user(s) **1**, secret from other parties (e.g., by memorizing same and recording same nowhere but in the mind(s) of such user(s) **1**).

[0054] Member ID(s) may be recorded not only in the mind(s), for example, of user(s) **1** but also at database(s) **4** belonging to verification facilitating system(s) **3**. That is, user(s) **1** and verification facilitating system(s) **3** (verification facilitating company X) may both possess such member ID(s). In such case, the only party other than user(s) **1** aware of the member ID(s) is verification facilitating system(s) **3** (verification facilitating company X).

[0055] Password(s) may be recorded not only in the mind(s), for example, of user(s) **1** but also at database(s) **7** belonging to verifying system(s) **6**. That is, user(s) **1** and verifying system(s) **6** (verifying company Y) may both possess such password(s). In such case, the only party other than user(s) **1** aware of the password(s) is verifying system(s) **6** (verifying company Y).

[0056] Accordingly, verification facilitating system(s) **3** (verification facilitating company X) knows or know the member ID(s) of such user(s) **1** but do not know the password(s) thereof. Conversely, verifying system(s) **6** (verifying company Y) knows or know the password(s) but do not know the member ID(s). In such case, the only party or parties aware of both keys or sets of keys unique to the user(s) **1** is or are the user(s) **1**. Apart from the user(s) **1**, only verification facilitating system(s) **3** (verification facilitating company X) and verifying system(s) **6** (verifying company Y), which constitute separate systems or sets of systems (organizations or sets of organizations), respectively or separately keep the member ID(s) and password(s) in mutually isolated fashion. Verification facilitating system(s) **3** (verification facilitating company X) and verifying system(s) **6** (verifying company Y) may respectively manage member ID(s) and password(s) such that they are separate and secret, one system or set of systems (organization or set of organizations) not revealing its key or keys to the other system or set of systems (organization or set of organizations).

[0057] Such separate, secret, and isolated management of the two types of keys belonging to the user(s) **1** permits improved reliability, which is to say security, in the verification of identity or identities of user(s) **1**, as described in further detail below. Furthermore, to link these two types of keys, managed as has been described so as to be mutually isolated, a third type of key may be employed. Such third key or keys, being temporary, session, or single-use key(s), may be referred to as "one-time ID(s)" in the present specification, and such one-time key(s) may be issued by verification facilitating system(s) **3** on demand by user(s) **1**.

[0058] Note that while **FIG. 1** only shows a single verifying company Y, there may in general be a plurality of such companies, and as noted elsewhere the singular is employed herein without intention to preclude presence of a plurality of same. Furthermore, regardless of whether there are a plurality of such verifying companies Y, there may be a plurality of verification facilitating companies X or there may be only a single verification facilitating company X (while there may of course be a plurality of such verification facilitating companies X, for convenience of description the present specification treats the case of verification of identity as facilitated by a single verification facilitating company X).

[0059] An exemplary sequence of operations for verifying identity using member ID(s), password(s), and one-time ID(s) is described below. In the present example, this sequence of operations can be divided into roughly two parts.

[0060] In the first part, shown in the top half of **FIG. 1**, preliminary first-stage identity check(s) of party or parties purporting to be user(s) **1** may be carried out by verification facilitating system(s) **3** using member ID(s), and in the present example, identification number(s) of mobile telephone(s) belonging to user(s) **1** (whereas telephone number(s) of mobile telephone(s) are used in the present example, other types of identifying code(s) associated with such mobile telephone(s) may alternatively or additionally be employed). In the event of positive verification of identity as a result of such preliminary identity check(s), verification facilitating system(s) **3** may issue one-time ID(s). Such one-time ID(s) may be communicated to both user(s) **1** and verifying system(s) **6**.

[0061] That is, in this first part of the present exemplary sequence of operations, user(s) **1** might use mobile telephone(s) **2** belonging to such user(s) **1** to place call(s) to verification facilitating system(s) **3**. Such verification facilitating system(s) **3** might automatically answer such call(s) and might compare telephone number(s) of originating party or parties (the telephone number(s) of the mobile telephone(s) **2**) to a list of telephone number(s) of member(s) (party or parties authorized to use the system(s) in question) registered in database(s) **4**. If as a result of such comparison it is determined that telephone number(s) of originating party or parties matches or match telephone number(s) of registered member(s), verification facilitating system(s) **3** might send to mobile telephone(s) **2** of user(s) **1** service menu(s) (e.g., in the form of voice prompts) prepared for user(s) **1**. User(s) **1** might use numeric keypad(s) (or voice

recognition functionality) of mobile telephone(s) **2** to select desired service(s) offered by desired verifying company or companies Y (e.g., credit transaction processing service(s) offered by credit service company or companies) and to enter member ID(s) of such user(s) **1** as prompted by such service menu(s), upon which such member ID(s) might be sent to verification facilitating system(s) **3**. Such verification facilitating system(s) **3** might compare such received member ID(s) with member ID(s) for member(s) registered in database(s) **4** found as described above as a result of match or matches with originating telephone number(s), and might determine, at least for the present purposes, that user(s) **1** is or are in fact the member(s) they purport to be if received member ID(s) matches or match the corresponding member ID(s) recorded in database(s) **4** for the party or parties having the originating telephone number(s). Upon making such determination, verification facilitating system(s) **3** might issue one-time ID(s) and might communicate such one-time ID(s) to mobile telephone(s) **2** of user(s) **1**, and might moreover communicate such one-time ID(s) to verifying system(s) **6** of desired verifying company or companies Y selected by user(s) **1** from service menu(s). The one-time ID(s) referred to here is or are unique data capable of being distinguished from other one-time ID(s) handled or likely to be handled by verification facilitating system(s) **3** and verifying system(s) **6**.

[0062] Furthermore, included among the data present for each member registered in database(s) **4** of verification facilitating system(s) **3** there may be, in addition to the aforementioned member ID(s) and telephone number(s) of mobile telephone(s), unique ID(s) (hereinafter "management master ID(s)") assigned to that member so as to permit identification of that member by verifying system(s) **6**, in which case verification facilitating system(s) **3** may, when communicating to verifying system(s) **6** the one-time ID(s) issued to user(s) **1**, also together therewith communicate to verifying system(s) **6** the management master ID(s) of the user(s) **1** (i.e., management master ID(s) of member(s) matched to originating telephone number(s) at the foregoing first-stage identity check(s)). This will permit verifying system(s) **6** to determine which member(s) was or were issued the one-time ID(s) communicated thereto. Verifying system(s) **6** may save one-time ID(s) communicated thereto in database(s) **7** as one-time ID(s) for the member(s) to which it or they was or were issued. For each respective member capable of using verifying system(s) **6**, then, management master ID(s) and password(s) may be registered in advance at database(s) **7** of verifying system(s) **6**, and one-time ID(s) may furthermore be registered therein as it or they is or are issued, as described above.

[0063] In this second part of the present exemplary sequence of operations, shown in the bottom half of **FIG. 1**, second-stage identity check(s) of party or parties purporting to be user(s) **1** may in the present example be carried out by verifying system(s) **6** using one-time ID(s) issued to user(s) **1** and password(s) unique to user(s) **1**.

[0064] That is, in the second part of the present exemplary sequence of operations, in order to receive the aforementioned desired service(s), user(s) **1** might use suitable terminal(s) **5** to send one-time ID(s) and password(s) of user(s) **1** from such terminal(s) **5** to verifying system(s) **6** of verifying company or companies Y. What is here referred to as suitable terminal(s) **5** might, for example if user(s) **1** attempts or attempt to use credit transaction processing service(s) to purchase goods at certain store(s), correspond to POS terminal(s) present at the store(s); or if user(s) **1** attempts or attempt to log on to certain server(s) from personal computer(s) belonging to user(s) **1**, correspond to such personal computer(s). Moreover, the person(s) directly operating such terminal(s) **5** need not be the user(s) **1**; other person(s), such as employee(s) at store(s), may alternatively or additionally perform such operations. Note that at time(s) when one-time ID(s) and/or password(s) of user(s) **1** is or are sent to verifying system(s) **6**, supplemental information to further improve processing to verify identity or as required to carry out processing in connection with service(s) to be provided subsequent to processing to verify identity, such as for example store ID(s) of the aforementioned store(s), might also typically be sent to verifying system(s) **6** together therewith.

[0065] Upon receipt of one-time ID(s) and password(s) of user(s) **1**, verifying system(s) **6** might search through sets of one-time ID(s) and password(s) for various member(s) already stored in database(s) **7** to see if there is or are set(s) which match received one-time ID(s) and password(s). If as a result of such search, set(s) of one-time ID(s) and password(s) of certain member(s) matches or match received one-time ID(s) and password(s), verifying system(s) **6** might determine, at least for the present purposes, that user(s) **1** is or are in fact the member(s) they purport to be, in which case the result of such search would be that positive identification(s) has or have been made. In the event that positive identification(s) has or have thus been made, the aforementioned desired service(s) might then be provided to user(s) **1** (e.g., processing of credit transaction(s) might be carried out, permission might be granted to log on to server(s), etc.).

[0066] If on the other hand it is found as a result of the foregoing procedure that no set of one-time ID(s) and password(s) for member(s) within database(s) **7** matches received one-time ID(s) and password(s), the result of such search might be that positive identification has not been made, in which case the aforementioned desired service(s) might not be provided to user(s) **1**.

[0067] Addressing again the situation where positive identification(s) has or have been made, in such a case verifying system(s) **6** might assign a "used" status to one-time ID(s) within database(s) **7** which was or were used in making such positive identification(s), and might moreover report to verification facilitating system(s) **3** that such one-time ID(s) has or have been used. Processing may be such that "used" one-time ID(s) is not or are not able to be used again for verification of identity (e.g., until passage of a sufficiently long period of time as described below). Addressing again the situation where positive identification has not been made, processing may in such a case be such that verifying system(s) **6** would not in general assign a "used" status to any one-time ID within database(s) **7**. Furthermore, processing may be such that one-time ID(s) expires or expire if not used by certain time(s), in which case verifying system(s) **6** might assign an "expired" status to such one-time ID(s) within database(s) **7** upon passage of such time(s) regardless of whether it or they has not or have not been used in making any positive identification, and might moreover report to verification facilitating system(s) **3** that such one-time ID(s) is or are expired. Processing may be such that "used" one-time ID(s) and/or "expired" one-time ID(s) does not or

do not become available to be issued again for use in verification of identity until passage of a sufficiently long period of time (i.e., such one-time ID(s) might again be made available for issuing only after sufficient time has passed—e.g., 1 year, 3 years, or the like—to substantially eliminate the likelihood of any compromise in security or reliability due to proximity in time to the previous issuance of such one-time ID(s)). In such case, the only one-time ID(s) which would in general be available for use in verification of identity would therefore be one-time ID(s) that is or are neither "used" nor "expired."'Used" one-time ID(s) and/or "expired" one-time ID(s) may however be subsequently used to assist in detection of fraudulent or accidental attempts at repeated use of one-time ID(s).

[0068] **FIG. 2** shows an example of a procedure by which user(s) **1** might register his, her, its, and/or their key(s) or the like with verification facilitating system(s) and/or verifying system(s).

[0069] Referring to **FIG. 2**, as indicated at step ①, user(s) **1** might use mobile telephone(s) **2** belonging to such user(s) **1** to place call(s) to verifying system(s) **6** of desired verifying company or companies Y (or might communicate therewith via other suitable method(s) such as written correspondence, WWW service(s), or the like), requesting registration as member(s). When making such request(s), in addition to street address(es), name(s), birth date(s), and/or other item(s) ordinarily provided on application(s) for membership or the like to permit access to desired service(s) or the like, user(s) **1** might also communicate originating telephone number(s) (e.g., telephone number(s) of mobile telephone(s) **2**) and password(s) of such user(s) **1** to verifying system(s) **6** (note that where communication to verifying system(s) **6** is via mobile telephone(s) **2**, the originating telephone number(s) thereof might ordinarily be communicated thereto automatically). If the information supplied on the application(s) by user(s) **1** is sufficient to satisfy condition(s) for membership or the like, verifying system(s) **6**, in registering user(s) **1** as member(s) thereof, might assign unique management master ID(s) to user(s) **1** and might record such management master ID(s), such originating telephone number(s) and password(s), and any such foregoing item(s) ordinarily provided on application(s) for membership, in database(s) **7** as member data unique to such user(s) **1**.

[0070] At step ②, verifying system(s) **6** might communicate such management master ID(s) and originating telephone number(s), and only such minimal information—e.g., names(s)—present among any such foregoing item(s) ordinarily provided on application(s) for membership as is or are necessary for facilitating verification (other personal information, e.g., street address(es), contact information, and the like, being omitted in the interest of preserving confidentiality of personal information) registered for such user(s) **1** to verification facilitating system(s) **3** of verification facilitating company X. In such case, password(s) of user(s) **1** is or are kept secret by verifying system(s) **6**, not being communicated to verification facilitating system(s) **3**.

[0071] At step ③, user(s) **1** might use mobile telephone(s) **2** belonging to such user(s) **1** to place call(s) to verification facilitating system(s) **3** (or might answer call(s) placed by verification facilitating system(s) **3** to mobile telephone(s) **2** belonging to such user(s) **1**) to confirm selection of such verifying company or companies Y and any such foregoing item(s) ordinarily provided on application(s) for membership, and might moreover communicate originating telephone number(s) (telephone number(s) of mobile telephone(s) **2**) and member ID(s) of such user(s) **1** to verification facilitating system(s) **3** by way of such mobile telephone(s) **2** (note that where user(s) **1** places or place call(s) to verification facilitating system(s) **3** from mobile telephone(s) **2**, the originating telephone number(s) thereof might ordinarily be communicated to such verification facilitating system(s) **3** automatically; and where verification facilitating system(s) **3** places or place call(s) to mobile telephone(s) **2**, confirmation of the fact that the answering party or parties is or are user(s) **1** might per force be taken as confirmation of such originating telephone number(s)). As a result of such telephonic or like communication with such user(s) **1**, verification facilitating system(s) **3** may be able to confirm correctness of originating telephone number(s) and any such foregoing item(s) ordinarily provided on application(s) for membership, and may consequently, in registering user(s) **1** as member(s) thereof, record in database(s) **4** as member data unique to such user(s) **1** such originating telephone number(s), management master ID(s), and any such foregoing item(s) ordinarily provided on application(s) for membership of such user(s) **1**. In such case, member ID(s) of user(s) **1** is or are kept secret by verification facilitating system(s) **3**, not being communicated to verifying system(s) **6**.

[0072] Examples of application of this embodiment to a number of specific uses are described below.

[0073] As a first example of application of the present embodiment, **FIG. 3** shows an application in the context of verification of identity such as might be carried out during processing of credit transaction(s).

[0074] In such case, as shown in **FIG. 3**, verifying company or companies Y might correspond to credit service company or companies used by user(s) **1**, and verifying system(s) **6** might correspond to computer system(s) belonging to such credit service company or companies.

[0075] Referring to **FIG. 3**, at time(s) when user(s) **1** wishes or wish to pay for purchase of goods at store(s) Z by means of credit transaction(s), user(s) **1** might, at step ①, place call(s) to verification facilitating system(s) **3** from mobile telephone(s) **2** belonging to such user(s) **1**. Upon so doing, verification facilitating system(s) **3** might recognize which member(s) is or are placing call(s) based on originating telephone number(s) of mobile telephone(s) **2**, and might return to such mobile telephone(s) **2** service menu(s) (e.g., voice prompts) designed for such member(s). User(s) **1** might operate mobile telephone(s) **2** as prompted by such service menu(s), communicating member ID(s) of such user(s) **1** and selected service(s) (e.g., selection of credit transaction processing service(s) by desired credit service company or companies Y) to verification facilitating system(s) **3**. Such verification facilitating system(s) **3** might compare member ID(s) communicated thereto from such purported user(s) **1** with member ID(s) of any member(s) recognized based on originating telephone number(s), and might determine, at least for the present purposes, that user(s) **1** is or are in fact the member(s) they purport to be in the event that such member IDs or sets of member IDs respectively match. Upon making such determination, veri-

fication facilitating system(s) **3** might, at step ②, issue to such user(s) **1** unique one-time ID(s) and might send same to mobile telephone(s) **2** of user(s) **1** and to verifying system(s) of credit service company or companies Y selected by user(s) **1** (in the example shown in the drawing, such verifying system(s) corresponds to system **6-1**, this being a system or set of systems associated with the company selected by the user **1**, and one of three systems or sets of systems **6-1** through **6-3** associated with three companies that all use the same verification facilitating company X). At such time(s), verification facilitating system(s) **3** might, together with such one-time ID(s), also send verifying system(s) **6-1** management master ID(s) assigned to such member(s) by such verifying system **6-1**. Verifying system(s) **6-1** might save such received one-time ID(s) in database **7-1** as one-time ID(s) for the member(s) corresponding to the received management master ID(s).

[0076] User(s) **1**, after receiving such issued one-time ID(s) at mobile telephone(s) **2** belonging to user(s) **1**, might, at step ③, enter one-time ID(s) and password(s) of such user(s) **1**—e.g., by manual input thereof—at POS terminal(s) **5** for processing of credit transaction(s) at store(s) Z. At step ④, such input one-time ID(s) and password(s) might be sent from POS terminal(s) **5** to verifying system(s) **6-1** of verifying company Y designated by user(s) **1**.

[0077] Upon receipt of such one-time ID(s) and password(s), verifying system(s) **6-1** might, at step ⑤, compare such received set(s) of one-time ID(s) and password(s) with set(s) of one-time ID(s) and password(s) for various member(s) present within database(s) **7-1**. If as a result of such comparison, set(s) of one-time ID(s) and password(s) of certain member(s) matches or match received one-time ID(s) and password(s), verifying system(s) **6-1** might determine, at least for the present purposes, that user(s) **1** is or are in fact the member(s) they purport to be (positive identification made). If on the other hand no member has a matching one-time ID and password set, verifying system(s) **6-1** might determine, at least for the present purposes, that user(s) **1** is not or are not the member(s) they purport to be (positive identification not made). Where positive identification(s) has or have been made, verifying system(s) **6-1** might use credit card information for user(s) **1** sent thereto from POS terminal(s) **5** to carry out credit transaction service processing. Where positive identification has not been made, verifying system(s) **6-1** might deny access to credit transaction processing service(s).

[0078] At step ⑥, verifying system(s) **6-1** might return to POS terminal(s) **5** the results of the foregoing identity check(s) (and/or results of any subsequent processing of credit transaction processing service(s)). At the foregoing second-stage identity check(s), verifying system(s) **6-1** might assign a "used" status to one-time ID(s) of user(s) **1** which was or were used here, preventing same from being used again for verification of identity before expiration of some sufficiently long time as described above.

[0079] As a second example of application of the present embodiment, **FIG. 4** shows an application in the context of verification of identity such as might be carried out when logging on to certain server(s).

[0080] In such case, as shown in **FIG. 4**, verifying company or companies Y might correspond to system operating company or companies operating server(s) used by user(s) **1**, and verifying system(s) **6** might correspond to such server(s).

[0081] At steps ①through ②in **FIG. 4**, operations through issuance of one-time ID(s) might be similar in principle to operations already described with reference to **FIG. 3**, the differences being that the service selected for use by user(s) **1** from service menu(s) is logging on to desired server(s) **6**, and the one-time ID(s) are sent to such server(s) **6**.

[0082] After issuance of one-time ID(s), user(s) **1**, at step ③, might enter such one-time ID(s) and password(s) of such user(s) **1**—e.g., by manual input thereof—at terminal(s) **5** for logging on to desired server(s) **6** (e.g., personal computer(s) belonging to user(s) **1**). Such entered one-time ID(s) and password(s) might be sent to server(s) **6**.

[0083] At steps ④ through ⑤, processing in connection with identity check(s) carried out at server(s) **6** using one-time ID(s) and password(s) might be similar in principle to processing in connection with identity check(s) already described with reference to steps ⑤through ⑥in **FIG. 3**, the difference being that permission to log on to server(s) **6** is granted instead of credit transaction processing being performed if positive identification(s) is or are made as a result of the identity check(s).

[0084] As a third example of application of the present embodiment, **FIG. 5** shows an application in the context of verification of identity such as might be carried out when certificatory document(s) issued by a local authority or the like is or are presented to user(s) **1**.

[0085] In such case, as shown in **FIG. 5**, verifying company or companies Y might correspond to such local authority or the like presenting such certificatory document(s) to user(s) **1**, and verifying system(s) **6** might correspond to document issuing system(s) associated with such local authority or the like. Furthermore, in the present example, special measures have been adopted that make it possible for the transaction to be completed without the need for user(s) **1** to disclose his, her, its, and/or their member ID(s) and/or password(s) to the other party or parties involved in the transaction when such certificatory document(s) is or are presented.

[0086] At steps ①through ②in **FIG. 5**, operations through issuance of one-time ID(s) might be similar in principle to operations already described with reference to **FIG. 3**, the differences being that the service selected for use by user(s) **1** from service menu(s) is the desired document issuing service offered by the local authority or the like, and the one-time ID(s) are sent to document issuing system(s) (verifying system(s) **6**) associated with such local authority or the like Y selected by user(s) **1**.

[0087] After issuance of one-time ID(s), user(s) **1**, at step ③, might cause one-time ID(s) and password(s) of such user(s) **1** to be input to document issuing system(s) (verifying system(s) **6**) associated with such local authority or the like Y and might request issuance of desired document(s) therefrom.

[0088] At step ④, document issuing system(s) might use one-time ID(s) and password(s) received from user(s) **1** to carry out identity check(s) on user(s) **1**, in which case processing in connection with such identity check(s) might

be similar in principle to processing in connection with identity check(s) performed by verifying system(s) of credit service company at step ⑤ in **FIG. 3**.

[0089] At step ⑤, if positive identification(s) is or are made as a result of such identity check(s), document issuing system(s) **6** might print out the requested certificatory document(s). At such time(s), document issuing system(s) **6** might issue document one-time ID(s) and might print out such document one-time ID(s) on such certificatory document(s). Such document one-time ID(s) might be unique to such certificatory document(s), permitting it or them to be distinguished from all other document one-time ID(s), and might furthermore be temporary or capable of only being used once. Such certificatory document(s) with attached document one-time ID(s) might after being printed out be delivered to user(s) **1**. Document issuing system(s) **6** might store such issued document one-time ID(s) in database(s) **7** as document one-time ID(s) of user(s) **1**. Furthermore, at time(s) when document one-time ID(s) is or are issued, document issuing system(s) **6** might assign a "document one-time ID(s) issued" status to one-time ID(s) of user(s) **1** but might not yet assign a "used" status thereto. Processing may be such that one-time ID(s) which has or have been assigned a "document one-time ID(s) issued" status would be prevented from being used again for identity check(s) in connection with document issuance at step ④, but would be capable of being used just once more, in third-stage identity check(s) at step ⑧, below, so long as it or they had not yet acquired a "used" status.

[0090] At step ⑥, user(s) **1** might present such certificatory document(s) to suitable company or companies Z making use of same (e.g., where such certificatory document(s) is or are being presented in order to conclude certain agreement(s) with company or companies, such company or companies serving as other party or parties to such agreement(s) might correspond to company or companies Z). At time(s) when such document(s) is or are presented, user(s) **1** might, at step ⑦, use terminal(s) **5** of company or companies Z to send one-time ID(s) of such user(s) **1** and document one-time ID(s) printed on such certificatory document(s) to document issuing system(s) **6** of local authority or the like Y.

[0091] Upon so doing, document issuing system(s) **6** might, at step ⑧, compare set(s) of one-time ID(s) and document one-time ID(s) for user(s) **1** received from terminal(s) **5** with set(s) of one-time ID(s) and document one-time ID(s) for various member(s) within database(s) **7**. If as a result of such comparison, set(s) of one-time ID(s) and document one-time ID(s) of certain member(s) matches or match received one-time ID(s) and document one-time ID(s), document issuing system(s) **6** might determine that positive identification(s) has or have been made; or if there is no such match, might determine that positive identification has not been made. Furthermore, where positive identification(s) has or have been made, document issuing system(s) **6** might assign a "used" status to set(s) of one-time ID(s) and document one-time ID(s) of user(s) **1** used therefor, preventing such set(s) from being used again for verification of identity.

[0092] In addition, at step ⑨, document issuing system(s) **6** might return to terminal(s) **5** of company or companies Z the results of the foregoing identity check(s). In the event that returned result(s) of identity check(s) indicate that positive identification(s) has or have been made, because this means that local authority or the like Y has confirmed that user(s) **1** is or are in fact the person(s) they purport to be, and moreover, that the certificatory document(s) was or were in fact issued to such person(s), company or companies Z can accept the certificatory document(s) from user(s) **1** with confidence.

[0093] Furthermore, from the standpoint of user(s) **1**, the fact that his, her, its, and/or their secret member ID(s) and password(s) have not been divulged to company or companies Z is beneficial for security.

[0094] As a fourth example of application of the present embodiment, **FIG. 6** shows an application in the context of verification of identity such as might be carried out during processing of credit transaction(s) when making purchase(s) over the Internet from web merchant(s) (website(s)).

[0095] In such case, as shown in **FIG. 6**, verifying company or companies Y might correspond to credit service company or companies used by user(s) **1**, and verifying system(s) **6** might correspond to verifying system(s) belonging to such credit service company or companies. Furthermore, in the present example, special measures have been adopted that make it possible for the transaction to be completed without the need for user(s) **1** to disclose his, her, its, and/or their credit card information to web merchant(s).

[0096] At steps ①through ②in **FIG. 6**, operations through issuance of one-time ID(s) are similar in principle to operations already described with reference to **FIG. 3**.

[0097] After issuance of one-time ID(s), user(s) **1**, at step ③, might use mobile telephone(s) **2** belonging to such user(s) **1** to place call(s) to verifying system(s) **6-1** of credit service company or companies Y selected by such user(s) **1**, and might send to such verifying system(s) **6-1** one-time ID(s) and password(s) of such user(s) **1** as well as store number(s) (shop ID(s)) of web merchant(s) **9** which such user(s) **1** desire to use.

[0098] At step ④, verifying system(s) **6-1** might use one-time ID(s) and password(s) received from user(s) **1** to carry out identity check(s) on user(s) **1** in accordance with a procedure similar to that described with reference to step ⑤ in **FIG. 3**. If positive identification(s) is or are made as a result of such identity check(s), verifying system(s) **6-1** might, at step ⑤, issue credit one-time ID(s) and might send such credit one-time ID(s) to mobile telephone(s) **2** of user(s) **1**. Such credit one-time ID(s) might be unique to a particular credit card or set of credit cards used by such user(s) **1**, permitting it or them to be distinguished from all other credit one-time ID(s), and might furthermore be temporary or capable of only being used once. Verifying system(s) **6-1** might store such issued credit one-time ID(s) and such store number(s) (shop ID(s)) received from such user(s) **1** in database(s) **7-1** as credit one-time ID(s) and store number(s) (shop ID(s)) corresponding to such user(s) **1**. Furthermore, at time(s) when credit one-time ID(s) is or are issued, verifying system(s) **6-1** might assign a "credit one-time ID(s) issued" status to one-time ID(s) of user(s) **1** but might not yet assign a "used" status thereto. Processing may be such that one-time ID(s) which has or have been assigned a "credit one-time ID(s) issued" status would be prevented from being used again for identity check(s) in connection

with credit one-time ID issuance at step ④, but would be capable of being used just once more, in third-stage identity check(s) at step ⑧, below, so long as it or they had not yet acquired a "used" status.

[0099] At step ⑥, user(s) **1** might use suitable terminal(s) **5** capable of connecting to the Internet (e.g., personal computer(s) belonging to user(s) **1**) to connect to web merchant(s) **9** (fresh connection to web merchant(s) **9** would of course not need to be established if connection thereto was made at previous time(s) and has not been broken), and might send one-time ID(s) and credit one-time ID(s) of such user(s) **1**—e.g., by manual input thereof—from such terminal(s) **5** to such web merchant(s) **9**. At step ⑦, web merchant(s) **9** might send such one-time ID(s) and credit one-time ID(s) from user(s) **1** as well as its or their own store number(s) (shop ID(s)) to verifying system(s) **6-1**.

[0100] At step ⑧, verifying system(s) **6-1** might compare set(s) of one-time ID(s) and credit one-time ID(s) and store number(s) (shop ID(s)) for such user(s) **1** received from web merchant(s) **9** with set(s) of one-time ID(s) and credit one-time ID(s) and store number(s) (shop ID(s)) for various member(s) within database(s) **7-1**. If as a result of such comparison, set(s) of one-time ID(s) and credit one-time ID(s) and store number(s) (shop ID(s)) of certain member(s) matches or match received one-time ID(s) and credit one-time ID(s) and store number(s) (shop ID(s)), verifying system(s) **6-1** might determine that positive identification(s) has or have been made; or if there is no such match, might determine that positive identification has not been made. Where positive identification(s) has or have been made, verifying system(s) **6-1** might use credit card information for user(s) **1** (i.e., member(s) found as a result of match(es) at the foregoing comparison) previously registered in database(s) **7-1** to carry out credit transaction service processing. Where positive identification has not been made, verifying system(s) **6-1** might deny access to credit transaction processing service(s). Furthermore, where such positive identification(s) has or have been made, verifying system(s) **6-1** might assign a "used" status to set(s) of one-time ID(s) and credit one-time ID(s) of user(s) **1** used therefor, preventing such set(s) from being used again for verification of identity.

[0101] At step ⑨, verifying system(s) **6-1** might return to web merchant(s) **9** the results of the foregoing identity check(s) (and/or results of processing of credit transaction processing service(s)).

[0102] In the present application of the present embodiment, because user(s) **1** need not send his, her, its, and/or their secret member ID(s) and password(s) and credit card information out over the Internet, such information not even being divulged to web merchant(s) **9**, web shopping can be carried out with confidence.

[0103] As a fifth example of application of the present embodiment, **FIG. 7** shows a variation in which encryption processing is added to the application in the context of logging on to server(s) shown in **FIG. 4**. At **FIG. 7**, underlining is used to indicate encrypted data.

[0104] Description of the variation shown in **FIG. 7** will focus primarily on those aspects which differ from the exemplary application shown in **FIG. 4**.

[0105] Mobile telephone(s) **2** of user(s) **1** may possess encryption and/or decryption capability. At step ②, verification facilitating system(s) **3** might use member ID(s) (first key(s)) from user(s) **1** to encrypt one-time ID(s) before sending same to mobile telephone(s) **2** of user(s) **1**. Upon receiving such encrypted one-time ID(s) at mobile telephone(s) **2**, user(s) **1** might enter his, her, its, and/or their member ID(s) (first key(s)) at mobile telephone(s) **2**, using such member ID(s) to decrypt such one-time ID(s) by means of decryption capability present at mobile telephone(s) **2**. At step ③, user(s) **1** might enter his, her, its, and/or their password(s) (second key(s)) at mobile telephone(s) **2**, using such password(s) (second key(s)) to encrypt such one-time ID(s) by means of encryption capability present at mobile telephone(s) **2**.

[0106] At step ④, user(s) **1** might enter such encrypted one-time ID(s) at terminal(s) **5**—e.g., by manual input thereof—and might send same to server(s) **6**. At step ⑤, server(s) **6** might use respective password(s) of various member(s) within database(s) **7** to decrypt such encrypted one-time ID(s) received from user(s) **1**, and might then compare such respective decrypted one-time ID(s) to one-time ID(s) of member(s) corresponding to such respective password(s). If as a result of such comparison, one-time ID(s) of certain member(s) matches or match received one-time ID(s), server(s) **6** might determine that positive identification(s) has or have been made, in which case permission to log on might be granted; or if no one-time ID of any member matches received one-time ID(s), might determine that positive identification has not been made, in which case permission to log on might not be granted.

[0107] By thus respectively using member ID(s) and password(s) at respective stages during processing for verification of identity, and by encrypting and decrypting one-time ID(s), improved security is achieved with respect to theft of one-time ID(s) through electronic interception thereof or the like. Note that from the standpoint of security it is preferred that entry of member ID(s), password(s), and one-time ID(s) by user(s) **1** be done manually (i.e., it is preferred that user(s) **1** memorize same and manually enter each into the system(s) where required).

[0108] Such variation in which encryption and decryption processing is added as described with reference to **FIG. 7** may be applied not only to the exemplary application shown in **FIG. 4**, but also to the exemplary applications shown in **FIGS. 3, 5**, and **6**.

[0109] As a sixth example of application of the present embodiment, **FIG. 8** shows a variation in which facial composite processing is added to the application in the context of credit transaction processing shown in **FIG. 3**.

[0110] Description of the variation shown in **FIG. 8** will focus primarily on those aspects which differ from the exemplary application shown in **FIG. 3**.

[0111] Facial image data for each member might be previously stored within database(s) **4** of verification facilitating system(s) **3**. At step ②, verification facilitating system(s) **3** might issue image one-time ID(s), such image one-time ID(s) being composite image data wherein one-time ID(s) is or are combined with facial image data for user(s) **1** (e.g., composite image data wherein one-time ID(s) in the form of image(s) of character string(s) is or are superposed on facial image(s) of user(s) **1** as shown in the drawing, or composite image data wherein one-time ID(s) is or are embedded

through digital watermarking or some other method so as to be invisible to the naked eye on facial image(s)), and such image one-time ID(s) might be sent to mobile telephone(s) **2** of user(s) **1** and verifying system(s) **6-1** of user-selected credit service company or companies Y. Mobile telephone(s) **2** might be capable of displaying received image one-time ID(s) at display panel(s), permitting user(s) **1** to confirm his, her, its, and/or their facial image(s) by looking at same. Note that mobile telephone(s) **2** may be constituted so as to be capable of extracting and separating facial image(s) and one-time ID(s) of user(s) **1** from image one-time ID(s) and so as to be capable of separate display of facial image(s) and one-time ID(s) at such display(s).

[0112] At step ③, user(s) **1** might cause image one-time ID(s) (or alternatively only facial image portion(s) thereof) to be displayed at display panel(s) of mobile telephone(s) **2** and might show same to store staffperson(s), and/or might enter one-time ID(s) and password(s) of such user(s) **1**—e.g., by manual input thereof—at POS terminal(s) **5** of such store(s) and might send such one-time ID(s) and password(s) to verifying system(s) **6-1** of credit service company or companies Y. Subsequent operations in connection with verification of identity by verifying system(s) **6-1** are similar to those described with reference to the exemplary application shown in **FIG. 3**.

[0113] In the present variation, the fact that facial image(s) of user(s) **1** issued by verification facilitating company X may also be used for verification of identity permits attainment of improved reliability. Because combination of facial image(s) and one-time ID(s) may be carried out by verification facilitating company X each time one-time ID(s) is or are issued, likelihood of forgery thereof can be reduced.

[0114] Such use of facial image(s) is possible not only in the exemplary application shown in **FIG. 3**, but also in the exemplary applications shown in **FIGS. 4 through 6**. Furthermore, such use of facial image(s) may be employed in combination with encryption and decryption such as has been described with reference to **FIG. 7**.

[0115] Below, a number of examples are cited to demonstrate how the present embodiment may improve reliability.

[0116] **FIG. 9** shows a situation where a third party acquires a mobile telephone belonging to a user and uses same to pretend to be that user.

[0117] Referring to **FIG. 9**, such third party **11** might find, for example, misplaced mobile telephone **2** and use same to, at step b, connect to verification facilitating system **3**. At such time, because third party **11** cannot enter member ID(s) of the owner(s) of mobile telephone **2**, positive identification is not made at first-stage identity check(s) performed by verification facilitating system **3**, making it impossible for one-time ID(s) to be issued. Moreover, even if third party **11** somehow happens to come into possession of such member ID(s) and somehow manages get one-time ID(s) issued, because third party **11** is unable to enter password(s) of the owner(s) of mobile telephone **2** at step ③, positive identification is not made at second-stage identity check(s) performed by verifying system **6-1**.

[0118] Accordingly, in such situation where a third party **11** pretends to be a user, so long as the third party **11** does not know both the member ID(s) and password(s) of the user, such third party **11** will be unable to obtain positive identification during identity check(s). Since member ID(s) and password(s) are respectively managed in isolated fashion by verification facilitating company or companies X and credit service company or companies (verifying company or companies) Y, unlike the conventional situation where a single organization might manage sets of member ID(s) and password(s), it is extremely difficult for a third party to come into possession thereof As a result, high reliability in verification of identity is therefore permitted.

[0119] **FIG. 10** shows a situation where a store attempts to use a password of a user to defraud a credit service company.

[0120] Referring to **FIG. 10, a** store staffperson might attempt to reuse a password entered at some time in the past by user **1** at POS terminal **5**, such staffperson for example requesting disbursement of funds at step ④ from verifying system **6-1** of credit service company Y. But because such staffperson cannot enter one-time ID(s) issued to user **1**, positive identification is not made at second-stage identity check(s) performed by verifying system **6-1** at step ⑤, and such disbursement of funds is denied. Furthermore, even if such staffperson were to attempt to reuse a one-time ID entered at some time in the past by user **1** at POS terminal **5**, verifying system(s) **6-1** might immediately detect this as a fraudulent or accidental attempt at repeated use of a one-time ID as a result of comparison which it might perform between such reused one-time ID and any "used" one-time ID(s) within database **7-1** (and/or it is possible to confirm use by user **1** based on such "used" one-time ID(s)). Accordingly, such attempt to defraud the credit service company would fail.

[0121] **FIG. 11** shows a situation in which a key is acquired by a third party through electronic interception thereof.

[0122] Referring to **FIG. 11**, third party **12** might intercept communication occurring between user **1** and verification facilitating system **3** at steps ① through ②, allowing such third party **12** to gain possession of a one-time ID of user **1** (or a similar example might be a situation where third party **12** gains possession of the member ID in this fashion, and acquires the one-time ID in this or some other way). But even if third party **12** manages to use the stolen one-time ID before user **1**, because third party **12** does not know password(s) of user **1**, positive identification will not be made at second-stage identity check(s) of step ⑤.

[0123] **FIG. 12** shows another situation involving electronic interception by a third party.

[0124] Referring to **FIG. 12**, third party **12** might intercept communication occurring between POS terminal **5** and verifying system **6** at step ④, allowing such third party **12** to gain possession of a one-time ID and password of user **1**. But when third party **12** attempts to use the stolen one-time ID and password, because user **1** has already used that one-time ID this would represent repeated use of the same one-time ID, and positive identification will not be made at second-stage identity check(s) of step ⑤.

[0125] This completes general description of the present embodiment. Detailed description of particular aspects of the present embodiment follows.

[0126] **FIG. 13** shows the constitution of a database **4** that might be associated with a verification facilitating system **3**

of a verification facilitating company X. **FIG. 14** shows the constitution of a database **7** that might be associated with a verifying system **6** of a verifying company Y.

[0127] Referring to **FIG. 13**, database **4** of verification facilitating system **3** may contain management master table(s) **21** wherein the following may be registered separately for each member: management ID(s) (ID(s) assigned to respective member(s) for internal use by verification facilitating system(s) **3**), telephone number(s) (originating telephone number(s)) of mobile telephone(s), first key(s) (member ID(s)), and emergency first key(s) (emergency member ID(s)). As described below with reference to **FIG. 23**, emergency first key(s) (emergency member ID(s) as used herein refer to dummy member ID(s) prepared in anticipation of the possibility that member(s) might be forced to reveal his, her, its, and/or their member ID(s) (first key(s)) as a result of intimidation or other such criminal activity on the part of a third party or the like, the idea being that such dummy member ID(s) could be revealed to such third party instead of real member ID(s).

[0128] One or more verifying company tables **22**, **23** within which may be recorded information pertaining to verifying company or companies registered by that member may be present, in which case it or they may be linked to the data for each member in management master table(s) **21**. Whereas in the example shown in the drawing one such registered company table **22** contains data pertaining to one or more system operating companies used by the member, and another such registered company table **23** contains data pertaining to one or more credit service companies used by the member, the invention is of course not limited to the particular examples shown here. Each such verifying company table **22**, **23**, if present, may contain recorded therein, separately for each verifying company, identification code(s) for that verifying company and management master ID(s) assigned to the member by that verifying company. Moreover, one or more code tables **24**, **25** within which may be recorded information of a bibliographic nature, such as identification code(s), name(s), address(es) and so forth for that verifying company, may be present, in which case it or they may be linked to the data for each verifying company listed within verifying company table(s) **22**, **23**, if present.

[0129] Furthermore, one or more log tables **26** for one or more members may be present, in which case it or they may be linked to the data for each member in management master table(s) **21**, if present. Log table(s) **26** for each member may, if present, contain recorded therein the member's management ID(s) and access log(s) logging access(es) to verification facilitating system(s) **3** (e.g., access start time period(s), input first key(s) (member ID(s)), time(s) required for input, verifying company or companies, management master ID(s), issued one-time ID(s), issue time(s), time(s) sent to verifying company or companies, status(es) at access end time(s), etc.).

[0130] Referring to **FIG. 14**, database **7** of verifying system **6** may contain verification management master table(s) **31** wherein the following may be registered separately for each member: the member's internal administrative purpose ID(s) (ID(s) assigned to the member and used only for an internal administrative purpose by verifying system(s)), management master ID(s), telephone number(s) (originating telephone number(s)) of mobile telephone(s), second key(s) (password(s)), and so forth.

[0131] One or more log tables **32** for one or more members may be present, in which case it or they may be linked to the data for each member in verification management master table(s) **31**. Log table(s) **32** for each member may, if present, contain recorded therein the member's internal administrative purpose ID(s) and management master ID(s) and access log(s) logging access(es) to verifying system(s) **6** (e.g., one-time ID(s) received, time(es) of receipt thereof, credit one-time ID(s) and/or document one-time ID(s) received, access time(s), second key(s) (password(s)) received, status(es) at access end time(s), etc.).

[0132] In addition, data for each member within verification management master table(s) **31**, if present, may be linked to data **33** (e.g., the member's street address(es), name(s), contact information, information pertaining to financial institution(s) for processing of transactions, credit card number(s), and/or other information necessary to carry out specific service(s) for that member such as processing of credit transactions) for that member within other database(s) belonging to such verifying company or companies.

[0133] **FIG. 15** shows an example of a service menu that might be provided to mobile telephone(s) **2** of user(s) **1** by verification facilitating system(s) **3**.

[0134] Whereas such service menu may as shown in **FIG. 15** for example have a hierarchical structure, being presented for example in the form of voice prompts, the invention is of course not limited to the particular example shown here, it being possible to present same by other methods (e.g., by display at display panel(s) of mobile telephone(s) **2**, etc.).

[0135] Referring to **FIG. 15**, such service menu may contain items for selection of various applications such as those described with reference to **FIGS. 3 through 6** (e.g., system operating companies carrying out login authentication, credit service companies carrying out verification for processing of credit transactions, document one-time ID issuance requests, credit one-time ID issuance requests, and/or other such selectable items). In addition, such service menu may contain items for selection of various useful functions such as those described below (e.g., service discontinuation requests, menu customization functionality, log display functionality, key management utilities, means for contacting owner in case misplaced mobile telephone is found by a third party, and/or other such selectable items).

[0136] **FIGS. 16 and 17** show specific sequences of operations that might occur at respective components in the context of an exemplary application involving processing of credit transaction(s) such as has been described with reference to **FIG. 3**, **FIG. 16** showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** and **FIG. 17** showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) **6**.

[0137] At **FIGS. 16 and 17**, steps enclosed in solid lines indicate operations that might be performed by user(s) **1**, and steps enclosed in dashed lines indicate operations that might be performed by system(s) associated with verification facilitating system(s) **3**, verifying system(s) **6**, or the like (the same convention applies to **FIGS. 18 through 29**).

[0138] Referring to **FIG. 16**, upon placement of a call by user **1** to verification facilitating system **3** using mobile

telephone **2** (step S1), verification facilitating system **3** compares the originating telephone number with originating telephone numbers registered to members (S2), and if a match is found, sends a service menu prepared for the matching member to mobile telephone **2** in the form of voice prompts (S3). These voice prompts prompt selection from among the service categories ("login", "credit", "other", etc.) present in the topmost level of the hierarchy of menu items shown in **FIG. 15**. User **1** selects "credit" from among those items (S4). Upon so doing, verification facilitating system **3** presents voice prompts for selection of a credit service company (S5), this representing a secondary menu level under "credit", and user **1** selects a desired credit service company (S6).

[0139] Verification facilitating system **3** then requests input of member ID from user **1** (S7), and user **1** enters his or her member ID at mobile telephone **2** and sends same to verification facilitating system **3**. Verification facilitating system **3** compares the member ID received from user **1** with the member ID registered to the member found as a result of the match described above (S9), and if these match, issues a one-time ID and sends same to mobile telephone **2** of user **1** (S11), and moreover sends that one-time ID and the management master ID of the user **1** (the member found as a result of the match above) to a verifying system **6** associated with the credit service company selected by the user **1** from the service menu (S12). The issued one-time ID is displayed at a display panel on mobile telephone **2** of user **1**.

[0140] Note that if a match is not found at step S2, verification facilitating system **3** carries out prescribed alternate processing (e.g., callback or the like) (S14). Furthermore, if a match is not found at step S9, verification facilitating system **3** carries out prescribed error processing (e.g., reprompt for member ID and carry out comparison again, or the like) (S15).

[0141] Referring to **FIG. 17**, when user **1**, after being issued the one-time ID, wants to use credit to purchase goods at a store (S21), user **1** enters his or her one-time ID and password at POS terminal **5** at the store (S22), and POS terminal **5** sends the input one-time ID and password, together with the store number (shop ID) of the store, to verifying system **6** of the credit service company (S23). Verifying system **6** compares the one-time ID-password set of user **1** received from POS terminal **5** with one-time ID-password sets registered to members (S24), and if a match is found, returns a message to POS terminal **5** to the effect that positive identification has been made and begins processing the credit transaction (or alternatively, processes the credit transaction and returns any results thereof to POS terminal **5**) (S25).

[0142] Note that if a match is not found at step S24, verifying system **6** carries out prescribed error processing (e.g., prompt user **1** for reentry of one-time ID, or the like) (S27).

[0143] **FIGS. 18 and 19** show specific sequences of operations that might occur at respective components in the context of an exemplary application involving logging on to server(s) such as has been described with reference to **FIG. 4**, **FIG. 18** showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3** and **FIG. 19** showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) (server(s)) **6**.

[0144] The following description focuses on those aspects of the sequences of operations at **FIGS. 18 and 19** which differ from the sequences of operations at **FIGS. 16 and 17**, described above.

[0145] Referring to **FIG. 18**, user **1** uses a service menu provided by verification facilitating system **3** to select the service category "login" and a desired system operating company (S34), and is issued a one-time ID (S36 through S38). The one-time ID and the management master ID of user **1** are communicated to server **6** (S34).

[0146] Referring to **FIG. 19**, upon entry of the one-time ID and a password at terminal **5** by user **1** (S52), terminal **5** sends the one-time ID and password, together with a terminal ID of that terminal **5**, to server **6**, whereupon server **6** compares the terminal ID with terminal IDs registered thereat (S53), and if a match is found, further compares the one-time ID-password set received from terminal **5** with one-time ID-password sets registered to members (S54), and if a match is found, determines that positive identification has been made, authorizing the login (S55).

[0147] **FIGS. 20 through 22** show specific sequences of operations that might occur at respective components in the context of an exemplary application involving issuance of certificatory document(s) by a local authority or the like such as has been described with reference to **FIG. 5**, **FIG. 20** showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) **3**, **FIG. 21** showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) (document issuing system(s)) **6**, and **FIG. 22** showing a sequence of operations in connection with third-stage identity check(s) that might be carried out by verifying system(s) (document issuing system(s)) **6**.

[0148] The following description focuses on those aspects of the sequences of operations at **FIGS. 20 through 22** which differ from the sequences of operations at **FIGS. 16 and 17**, described above.

[0149] Referring to **FIG. 20**, user **1** uses a service menu provided by verification facilitating system **3** to select the service category "other" and the subcategory "issuance of documents by local authority or the like" (S64, S66), and is issued a one-time ID (S67 through S70). The one-time ID and the management master ID of user **1** are communicated to document issuing system **6** associated with such local authority or the like (S71).

[0150] Referring to **FIG. 21**, user **1**, after being issued the one-time ID, submits a request for issuance of documents to a local authority or the like (S81), at which time user **1** informs the local authority or the like of his or her one-time ID and password (S82), whereupon a staffperson at the local authority or the like enters the one-time ID and password at the document issuing system **6** (S83) (or at steps S82 through S83, user **1** himself or herself enters the one-time ID and password at document issuing system **6**). Document issuing system **6** compares the one-time ID-password set received from user **1** with one-time ID-password sets registered to members (S84), and if a match is found, issues a

document one-time ID (S85) and prints out the certificatory documents, with the document one-time ID being moreover printed thereon (S86). User 1 receives the certificatory documents (S87).

[0151] Referring to FIG. 22, user 1 presents the certificatory documents to a prescribed company making use of same (S91, S92), and moreover informs this company of his or her one-time ID (S93), whereupon an employee of the company enters at terminal 5 of that company the one-time ID of the user 1 and the document one-time ID printed on the certificatory documents which were presented thereto and forwards same to document issuing system 6 of the local authority or the like (S94). Document issuing system 6 compares the set comprising the one-time ID of user 1 and the document one-time ID from the documents which were presented, this set having been received from terminal 5, with one-time ID-document one-time ID sets registered to members (S95), and if a match is found, returns a message to terminal 5 of the company to the effect that positive identification has been made (S96).

[0152] FIGS. 23 through 25 show specific sequences of operations that might occur at respective components in the context of an exemplary application involving processing of credit transaction(s) when making purchase(s) during web shopping such as has been described with reference to FIG. 6, FIG. 23 showing a sequence of operations in connection with first-stage identity check(s) that might be carried out by verification facilitating system(s) 3, FIG. 24 showing a sequence of operations in connection with second-stage identity check(s) that might be carried out by verifying system(s) 6 of credit service company or companies, and FIG. 25 showing a sequence of operations in connection with third-stage identity check(s) that might be carried out by verifying system(s) 6 of credit service company or companies.

[0153] The following description focuses on those aspects of the sequences of operations at FIGS. 23 through 25 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0154] Referring to FIG. 23, user 1 uses a service menu provided by verification facilitating system 3 to select the service category "other" and the subcategory "web purchase" (S104, S106), and is issued a one-time ID (S107 through S110).

[0155] Referring to FIG. 24, after being issued the one-time ID, user 1 uses his or her mobile telephone 2 to access verifying system 6 of a credit service company (S121). Verifying system 6 compares the originating telephone number of user 1 with originating telephone numbers registered to members (S122), and if a match is found, sends a service menu prepared for the matching member to mobile telephone 2 in the form of voice prompts (S123). These voice prompts prompt selection from among various types of transactions for which the user might desire processing as a credit transaction (e.g., electronic purchases or any of various other types of business transactions). User 1 selects "web purchase" from among those items (S124). Upon so doing, verifying system 6 presents voice prompts for selection among various web merchants which support credit transactions (S125), and user 1 selects a desired web merchant (S126).

[0156] Verifying system 6 then requests input of the one-time ID and password from user 1 (S127), and user 1 uses mobile telephone 2 to enter the one-time ID and password and store number of the web merchant and send same to verifying system 6 (S128). Verifying system 6 compares the one-time ID-password set which was input by user 1 with one-time ID-password sets registered to members (S129), and if a match is found, issues a credit one-time ID and sends same to mobile telephone 2 of user 1 (S130). The issued credit one-time ID is displayed at a display panel on mobile telephone 2 of user 1.

[0157] Referring to FIG. 25, after making a purchase from web merchant 9, user 1 proceeds to a web page at which he or she completes a procedure to initiate processing of an online transaction (S141), inputting his or her one-time ID and credit one-time ID at this online transaction processing web page (or alternatively sending these thereto via electronic mail) (S142). Web merchant 9 receives the one-time ID and credit one-time ID (S143), and forwards the one-time ID and credit one-time ID, together with the store number (shop ID) of same merchant, to verifying system 6 of a credit service company (S144). Verifying system 6 compares the one-time ID-credit one-time ID-store number set received from web merchant 9 with one-time ID-credit one-time ID-store number sets registered to members (S145), and if a match is found, informs web merchant 9 that positive identification has been made and begins processing the credit transaction (or alternatively, processes the credit transaction and informs web merchant 9 of the result) (S146).

[0158] FIG. 26 shows a sequence of operations that might occur during emergency communication using an emergency member ID and dummy verification processing.

[0159] Such emergency communication and dummy verification processing is an effective countermeasure which may be applied for example in the event that user 1 is forced to reveal his or her key(s) or to make a credit transaction as a result of intimidation or other such criminal activity.

[0160] The following description focuses on those aspects of the sequence of operations at FIG. 26 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0161] Referring to FIG. 26, upon being prompted by verification facilitating system 3 to enter his or her member ID (S157), user 1 enters an emergency member ID, acquired in advance in anticipation of such a possibility and different from his or her real member ID, at mobile telephone 2 and sends same to verification facilitating system 3 (S158). When verification facilitating system 3 receives an emergency member ID, since the result of the member ID comparison performed at step S159 will be that no match is found, processing will proceed to the error processing of step S165. During such error processing, verification facilitating system 3 compares the emergency member ID received from user 1 with the emergency member IDs registered to members (S166), and if a match is found, causes processing to proceed to step S160, where a one-time ID is issued in the same manner as with normal processing, and in addition causes processing to proceed to step S167, where information pertaining to user 1 is reported to the police or a security company or the like and appropriate action is requested therefrom, and where all credit service companies capable of being used by user 1 are furthermore requested to carry out processing to terminate ability of user

1 to use credit services. Note that if a match is not found at step S166, verification facilitating system 3 requests repeated communication from user 1 and terminates the communication (S169).

[0162] Since user 1 is able to obtain a one-time ID, user 1 uses that one-time ID to carry out procedures in connection with processing of the credit transaction in the same manner as described with reference to FIG. 17 (S171). At such time, verifying system 6 of the credit service company and the POS terminal of the store engage in operations that to all outward appearances make it seem to the user 1 and any onlooker that processing of the credit transaction is proceeding as usual, when in fact a report such as will allow appropriate crime prevention measures to be carried out is being made to store personnel, the police, a security company, or other such concerned parties (S172).

[0163] Because use of an emergency member ID thus makes it possible to give the appearance that positive identification has been made when in fact processing for crime prevention is being carried out in the background, it is possible to effectively stop criminal activity while protecting the security of user 1.

[0164] FIG. 27 shows a sequence of operations for discontinuing a service at the request of user 1.

[0165] The following description focuses on those aspects of the sequence of operations at FIG. 27 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0166] Referring to FIG. 27, after selecting "discontinue all services", "discontinue login services only", or "discontinue credit services only" under "discontinue service" under "other" from the service menu (see FIG. 15) provided by verification facilitating system 3 (S184, S186), user 1 enters his or her member ID (S188). If a match is found as a result of member ID comparison performed by verification facilitating system 3 at step S189, processing to discontinue all services (S190 through S194), processing to discontinue login services only (S195 through S198), or processing to discontinue credit services only (S199 through S202) is carried out in accordance with the selection of user 1. Regardless of which category of services is requested to be discontinued, all verifying companies (e.g., system operating companies, credit service companies, etc.) providing the service(s) to be discontinued are sent the respective company's management master ID for user 1 together with a request to discontinue service (S191, S197, or S201), and in addition, a "service discontinued" message is inserted in the service menu for that user 1 at the location(s) corresponding to the discontinued service(s) (S201).

[0167] FIG. 28 shows a sequence of operations in connection with menu customization functionality.

[0168] Menu customization functionality refers to the ability of user 1 to edit the order and otherwise customize presentation of menu items in a version of the service menu personalized for that user 1.

[0169] The following description focuses on those aspects of the sequence of operations at FIG. 28 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0170] Referring to FIG. 28, after selecting "customize menu" under "other" from the service menu (see FIG. 15) provided by verification facilitating system 3 (S215, S217), user 1 enters his or her member ID (S219). If a match is found as a result of member ID comparison performed by verification facilitating system 3 at step S220, voice prompts are presented to user 1 prompting selection of more detailed customization functionality—e.g., "rearrange menu categories", "rearrange company names", "turn voice prompts ON or OFF", "done", etc.—and user 1 selects a desired customization functionality therefrom (S221). Verification facilitating system 3 carries out processing in connection with the customization functionality selected by user 1; i.e., processing to rearrange menu categories (S223 through S225), processing to rearrange company names (S226 through S228), or processing to turn voice prompts ON or OFF (S229 through S231). Regardless of which category of customization functionality is selected, processing is such as to allow user 1 to specify what modifications he or she wants to make to the service menu (S224, S227, or S230). These modifications will be reflected in the way the service menu is presented the next time that it is accessed.

[0171] FIG. 29 shows a sequence of operations in connection with functionality for retrieving and displaying a log of websites of web merchants or the like which have been accessed.

[0172] The following description focuses on those aspects of the sequence of operations at FIG. 29 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0173] Referring to FIG. 29, after selecting "get log" under "other" from the service menu (see FIG. 15) provided by verification facilitating system 3 (S244, S246), user 1 enters his or her member ID (S248). If a match is found as a result of member ID comparison performed by verification facilitating system 3 at step S249, voice prompts are presented to user 1 prompting selection of the type of log to be retrieved—e.g., "i-mode" (a service mark of NTT DOCOMO LTD. registered in Japan for Internet providing services for cellular phone), "Web", "done", etc.—and user 1 selects a desired type of log therefrom (S250). Verification facilitating system 3 performs processing to retrieve the type of log selected by user 1 and to output it to a mobile telephone of user 1; i.e., processing to retrieve and display a log of websites accessed via i-mode (S252 through S254) or processing to retrieve and display a log of websites accessed via ordinary web browser (S255 through S257).

[0174] FIG. 30 shows a sequence of operations for changing key(s).

[0175] The following description focuses on those aspects of the sequence of operations at FIG. 30 which differ from the sequences of operations at FIGS. 16 and 17, described above.

[0176] Referring to FIG. 30, after selecting "change key" under "key-related tasks" under "other" from the service menu (see FIG. 15) provided by verification facilitating system 3 (S264, S266), user 1 enters his or her member ID (S268). If a match is found as a result of member ID comparison performed by verification facilitating system 3 at step S269, user 1 is prompted to enter a new member ID (first key) (S270, S272), and user 1 enters a new member ID

(S271, S273). Verification facilitating system **3** then replaces the member ID registered to user **1** at database **4** with the new member ID which was entered by user **1** (S275). Furthermore, if user **1** has also requested that his or her password (second key) be changed, verification facilitating system **3** informs verifying system **6** of such request. While not shown in the drawings, processing for changing the password, where requested, takes place through communication between user **1** and verifying system **6** without involvement of verification facilitating system **3**.

[0177] **FIG. 31** shows a sequence of operations for receiving confirmation of key content.

[0178] The following description focuses on those aspects of the sequence of operations at **FIG. 31** which differ from the sequences of operations at **FIGS. 16 and 17**, described above.

[0179] Referring to **FIG. 31**, user **1** selects "confirm keys" under "key-related tasks" under "other" from the service menu (see **FIG. 15**) provided by verification facilitating system **3** (S284, S286). Upon so doing, because verification facilitating company X does not know the street address or contact information of user **1**, verification facilitating company X prints out the member ID (first key) of user **1** which it places in a sealed envelope and sends to a credit service company or other such verifying company Y which does have such contact information for user **1** so as to permit such verifying company Y to inform user **1** of the content of his or her key(s) (S287). Verifying company Y prints out the password (second key) of user **1**, which it mails to user **1** together with the printed member ID (first key) that it received from verification facilitating company X (S288).

[0180] **FIG. 32** shows a sequence of operations for contacting the owner of misplaced mobile telephone which is found by a third party.

[0181] The following description focuses on those aspects of the sequence of operations at **FIG. 32** which differ from the sequences of operations at **FIGS. 16 and 17**, described above.

[0182] Referring to **FIG. 32, a** third party finding mobile telephone **2** uses that mobile telephone **2** to place a call to verification facilitating system **3** (S301), and selects "contact owner to report that misplaced mobile telephone has been found" under "other" from the service menu (see **FIG. 15**) provided by verification facilitating system **3** (S304, S306). Because verification facilitating company **3** does not know the street address or contact information of user **1**, verification facilitating company **3** informs a credit service company or other such verifying company Y which does have such contact information for user **1** of the fact that a lost mobile telephone has been found (S307), and verifying company Y, upon being so informed, carries out processing for receipt of the mobile telephone **2** from the person who found it and delivery of same to user **1** (S308).

[0183] Whereas several embodiments of the present invention and variations thereof have been described above, these examples have been presented merely for purposes of describing the invention and it not intended that the invention should be limited thereto. The present invention may be carried out in the context of a wide variety of modes and embodiments other than those specifically presented herein.

What is claimed is:

1. A method for verifying identity comprising:

a. a step wherein only first key or keys of one or more users possessing both first key or keys and second key or keys is or are saved by one or more first systems;

b. a step wherein only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved by one or more second systems;

c. a step wherein at least one of the first system or systems

i. receives input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and

ii. carries out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users;

d. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks, a step wherein at least one of the first system or systems causes one or more one-time IDs to be issued to at least one of the user or users;

e. a step wherein at least one of the first system or systems communicates to at least one of the second system or systems at least one of the one-time ID or IDs issued to at least one of the user or users;

f. a step wherein at least one of the second system or systems saves at least one of the one-time ID or IDs communicated thereto by the at least one first system;

g. a step wherein at least one of the second system or systems

i. receives input of data purporting to be at least one of the second key or keys and at least one of the one-time ID or IDs and

ii. carries out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved one-time ID or IDs of at least one of the user or users; and

h. a step wherein provision of one or more services to at least one of the user or users is controlled in correspondence to at least one result of at least one of the second-stage identity check or checks.

2. A method for verifying identity according to claim 1 further comprising:

a. a step wherein at least one of the first system or systems saves one or more identification numbers of one or more mobile communication terminals of at least one of the user or users;

b. the step at which one or more first-stage identity checks is or are carried out being such that

i. input of data purporting to be at least one of the first key or keys is received by way of one or more mobile

communication terminals from at least one of the party or parties purporting to be at least one of the user or users and

ii. at least one of the first-stage identity check or checks is carried out by comparing at least one of the input purported first key or keys and at least one identification number of at least one of the mobile communication terminal or terminals used for input thereof to at least one of the saved first key or keys and at least one of the saved identification number or numbers of at least one of the mobile communication terminal or terminals of at least one of the user or users.

3. A method for verifying identity according to claim 1 further comprising:

a. a step wherein at least one of the first system or systems saves one or more facial images of at least one of the user or users;

b. the step at which one or more one-time IDs is or are issued being such that, in addition to the one or more one-time IDs, at least one of the saved facial image or images of at least one of the user or users is issued to at least one of the user or users in such fashion as to permit display thereof by at least one of the user or users.

4. A method for verifying identity comprising:

a. a step wherein only first key or keys of one or more users possessing both first key or keys and second key or keys is or are saved by one or more first systems;

b. a step wherein only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved by one or more second systems;

c. a step wherein at least one of the first system or systems

i. receives input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and

ii. carries out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users;

d. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks, a step wherein at least one of the first system or systems causes one or more first one-time IDs to be issued to at least one of the user or users;

e. a step wherein at least one of the first system or systems communicates to at least one of the second system or systems at least one of the first one-time ID or IDs issued to at least one of the user or users;

f. a step wherein at least one of the second system or systems saves at least one of the first one-time ID or IDs communicated thereto by the at least one first system;

g. a step wherein at least one of the second system or systems

i. receives input of data purporting to be at least one of the second key or keys and at least one of the first one-time ID or IDs from one or more parties purporting to be at least one of the user or users and

ii. carries out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported first one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved first one-time ID or IDs of at least one of the user or users;

h. if at least one positive verification of identity is made at at least one of the second-stage identity check or checks, a step wherein at least one of the second system or systems causes one or more second one-time IDs to be issued to at least one of the user or users;

i. a step wherein at least one of the second system or systems

i. receives input of data purporting to be at least one of the first one-time ID or IDs and at least one of the second one-time ID or IDs and

ii. carries out one or more third-stage identity checks by comparing at least one of the input purported first one-time ID or IDs and at least one of the input purported second one-time ID or IDs to at least one of the saved first one-time ID or IDs and at least one of the saved second one-time ID or IDs of at least one of the user or users; and

j. a step wherein provision of one or more services to at least one of the user or users is controlled in correspondence to at least one result of at least one of the third-stage identity check or checks.

5. A system for verifying identity comprising:

a. one or more first systems that saves or save only first key or keys of one or more users possessing both first key or keys and second key or keys; and

b. one or more second systems that saves or save only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys;

c. at least one of the first system or systems comprising

i. means

1. for receiving input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and

2. for carrying out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users;

ii. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks, means for causing one or more one-time IDs to be issued to at least one of the user or users; and

iii. means for communicating at least one of the one-time ID or IDs issued to at least one of the user or users to at least one of the second system or systems;

d. at least one of the second system or systems comprising

i. means for saving at least one of the one-time ID or IDs communicated thereto by the at least one first system; and

ii. means

1. for receiving input of data purporting to be at least one of the second key or keys and at least one of the one-time ID or IDs and

2. for carrying out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved one-time ID or IDs of at least one of the user or users;

e. provision of one or more services to at least one of the user or users being capable of being controlled in correspondence to at least one result of at least one of the second-stage identity check or checks.

6. A system for verifying identity according to claim 5 wherein

a. the at least one first system further comprises means for saving one or more identification numbers of one or more mobile communication terminals of at least one of the user or users;

b. the means at the at least one first system for carrying out one or more first-stage identity checks being such that

i. input of data purporting to be at least one of the first key or keys is received by way of one or more mobile communication terminals from at least one of the party or parties purporting to be at least one of the user or users and

ii. at least one of the first-stage identity check or checks is carried out by comparing at least one of the input purported first key or keys and at least one identification number of at least one of the mobile communication terminal or terminals used for input thereof to at least one of the saved first key or keys and at least one of the saved identification number or numbers of at least one of the mobile communication terminal or terminals of at least one of the user or users.

7. A system for verifying identity according to claim 5 wherein

a. the at least one first system further comprises means for saving one or more facial images of at least one of the user or users;

b. the means at the at least one first system for issuing one or more one-time IDs being such that, in addition to the one or more one-time IDs, at least one of the saved facial image or images of at least one of the user or users is issued to at least one of the user or users in such fashion as to permit display thereof by at least one of the user or users.

8. A system for verifying identity comprising:

a. one or more first systems that saves or save only first key or keys of one or more users possessing both first key or keys and second key or keys; and

b. one or more second systems that saves or save only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys;

c. at least one of the first system or systems comprising

i. means

1. for receiving input of data purporting to be at least one of the first key or keys from one or more parties purporting to be at least one of the user or users and

2. for carrying out one or more first-stage identity checks by comparing at least one of the input purported first key or keys to at least one of the saved first key or keys of at least one of the user or users;

ii. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks, means for causing one or more first one-time IDs to be issued to at least one of the user or users; and

iii. means for communicating at least one of the first one-time ID or IDs issued to at least one of the user or users to at least one of the second system or systems;

d. at least one of the second system or systems comprising

i. means for saving at least one of the first one-time ID or IDs communicated thereto by the at least one first system;

ii. means

1. for receiving input of data purporting to be at least one of the second key or keys and at least one of the first one-time ID or IDs from one or more parties purporting to be at least one of the user or users and

2. for carrying out one or more second-stage identity checks by comparing at least one of the input purported second key or keys and at least one of the input purported first one-time ID or IDs to at least one of the saved second key or keys and at least one of the saved first one-time ID or IDs of at least one of the user or users;

iii. if at least one positive verification of identity is made at at least one of the second-stage identity check or checks, means for causing one or more second one-time IDs to be issued to at least one of the user or users; and

iv. means

1. for receiving input of data purporting to be at least one of the first one-time ID or IDs and at least one of the second one-time ID or IDs and

2. for carrying out one or more third-stage identity checks by comparing at least one of the input purported first one-time ID or IDs and at least one of the input purported second one-time ID or IDs to at least one of the saved first one-time ID or IDs and at least one of the saved second one-time ID or IDs of at least one of the user or users;

e. provision of one or more services to at least one of the user or users being capable of being controlled in correspondence to at least one result of at least one of the third-stage identity check or checks.

9. A method for facilitating verification of identity by one or more verifying systems that uses or use second key or keys of one or more users possessing both first key or keys and second key or keys to carry out verification of identity of one or more parties purporting to be at least one of the user or users, the method comprising:

a. step wherein only first key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved, at least one of the saved first key or keys being kept secret from at least one of the verifying system or systems;

b. a step wherein at least one of the saved first key or keys of at least one of the user or users is used to carry out one or more preliminary identity checks;

c. if at least one positive verification of identity is made at at least one of the preliminary identity check or checks, a step wherein one or more one-time IDs are issued to at least one of the user or users; and

d. a step wherein at least one of the one-time ID or IDs issued to at least one of the user or users is communicated to at least one of the verifying system or systems;

e. whereby at least one of the verifying system or systems is made capable of using at least one of the second key or keys and at least one of the one-time ID or IDs to verify identity of one or more parties purporting to be at least one of the user or users.

10. A method for facilitating verification of identity according to claim 9 further comprising:

a. a step wherein one or more identification numbers of one or more mobile communication terminals of at least one of the user or users is or are saved;

b. the step at which one or more preliminary identity checks is or are carried out being such that

i. communication is established with at least one of the party or parties purporting to be at least one of the user or users by way of one or more mobile communication terminals and,

ii. in addition to the at least one first key, at least one identification number of at least one of the mobile communication terminal or terminals used to establish the communication is used to carry out at least one of the preliminary identity check or checks.

11. A system for facilitating verification of identity by one or more verifying systems that uses or use second key or keys of one or more users possessing both first key or keys and second key or keys to carry out verification of identity of one or more parties purporting to be at least one of the user or users, the system comprising:

a. means for saving only first key or keys of at least one of the user or users possessing both first key or keys and second key or keys, at least one of the saved first key or keys being kept secret from at least one of the verifying system or systems;

b. means for using at least one of the saved first key or keys of at least one of the user or users to carry out one or more preliminary identity checks;

c. if at least one positive verification of identity is made at at least one of the preliminary identity check or checks, means for issuing one or more one-time IDs to at least one of the user or users; and

d. means for communicating at least one of the one-time ID or IDs issued to at least one of the user or users to at least one of the verifying system or systems;

e. whereby at least one of the verifying system or systems is made capable of using at least one of the second key or keys and at least one of the one-time ID or IDs to verify identity of one or more parties purporting to be at least one of the user or users.

12. A system for facilitating verification of identity according to claim 11 further comprising:

a. means for saving one or more identification numbers of one or more mobile communication terminals of at least one of the user or users;

b. the means for carrying out one or more preliminary identity checks being such that

i. communication is established with at least one of the party or parties purporting to be at least one of the user or users by way of one or more mobile communication terminals and,

ii. in addition to the at least one first key, at least one identification number of at least one of the mobile communication terminal or terminals used to establish the communication is used to carry out at least one of the preliminary identity check or checks.

13. A method for verifying identity as facilitated by one or more verification facilitating systems that uses or use first key or keys of one or more users possessing both first key or keys and second key or keys to carry out one or more first-stage identity checks of one or more parties purporting to be at least one of the user or users, the method comprising:

a. a step wherein only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved, at least one of the saved second key or keys being kept secret from at least one of the verification facilitating system or systems;

b. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks carried out by at least one of the verification facilitating system or systems, a step wherein one or more one-time IDs issued to at least one of the user or users is or are received from at least one of the verification facilitating system or systems;

c. a step wherein at least one of the one-time ID or IDs received from the verification facilitating system or systems is saved; and

d. a step wherein at least one of the saved second key or keys and at least one of the saved one-time ID or IDs of at least one of the user or users are used to carry out one or more second-stage identity checks of one or more parties purporting to be at least one of the user or users.

14. A system for verifying identity as facilitated by one or more verification facilitating systems that uses or use first key or keys of one or more users possessing both first key or keys and second key or keys to carry out one or more first-stage identity checks of one or more parties purporting to be at least one of the user or users, the system comprising:

a. means for saving only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys, at least one of the saved second key or keys being kept secret from at least one of the verification facilitating system or systems;

b. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks carried out by at least one of the verification facilitating system or systems, means for receiving from at least one of the verification facilitating system or systems one or more one-time IDs issued to at least one of the user or users;

c. means for saving at least one of the one-time ID or IDs received from the verification facilitating system or systems; and

d. means for using at least one of the saved second key or keys and at least one of the saved one-time ID or IDs of at least one of the user or users to carry out one or more second-stage identity checks of one or more parties purporting to be at least one of the user or users.

15. A method for verifying identity as facilitated by one or more verification facilitating systems that uses or use first key or keys of one or more users possessing both first key or keys and second key or keys to carry out one or more first-stage identity checks of one or more parties purporting to be at least one of the user or users, the method comprising:

a. a step wherein only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys is or are saved, at least one of the saved second key or keys being kept secret from at least one of the verification facilitating system or systems;

b. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks carried out by at least one of the verification facilitating system or systems, a step wherein one or more first one-time IDs issued to at least one of the user or users is or are received from at least one of the verification facilitating system or systems;

c. a step wherein at least one of the first one-time ID or IDs received from the verification facilitating system or systems is saved;

d. a step wherein at least one of the saved second key or keys and at least one of the saved first one-time ID or IDs of at least one of the user or users are used to carry out one or more second-stage identity checks of one or more parties purporting to be at least one of the user or users;

e. if at least one positive verification of identity is made at at least one of the second-stage identity check or checks, a step wherein

i. one or more second one-time IDs are issued to at least one of the user or users and

ii. at least one of the issued second one-time ID or IDs is saved; and

f. a step wherein at least one of the saved first one-time ID or IDs and at least one of the saved second one-time ID or IDs of at least one of the user or users are used to carry out one or more third-stage identity checks of one or more parties purporting to be at least one of the user or users.

16. A system for verifying identity as facilitated by one or more verification facilitating systems that uses or use first key or keys of one or more users possessing both first key or keys and second key or keys to carry out one or more first-stage identity checks of one or more parties purporting to be at least one of the user or users, the system comprising:

a. means for saving only second key or keys of at least one of the user or users possessing both first key or keys and second key or keys, at least one of the saved second key or keys being kept secret from at least one of the verification facilitating system or systems;

b. if at least one positive verification of identity is made at at least one of the first-stage identity check or checks carried out by at least one of the verification facilitating system or systems, means for receiving from at least one of the verification facilitating system or systems one or more first one-time IDs issued to at least one of the user or users;

c. means for saving at least one of the first one-time ID or IDs received from the verification facilitating system or systems;

d. means for using at least one of the saved second key or keys and at least one of the saved first one-time ID or IDs of at least one of the user or users to carry out one or more second-stage identity checks of one or more parties purporting to be at least one of the user or users;

e. if at least one positive verification of identity is made at at least one of the second-stage identity check or checks, means

i. for issuing one or more second one-time IDs to at least one of the user or users and

ii. for saving at least one of the issued second one-time ID or IDs; and

f. means for using at least one of the saved first one-time ID or IDs and at least one of the saved second one-time ID or IDs of at least one of the user or users to carry out one or more third-stage identity checks of one or more parties purporting to be at least one of the user or users.

* * * * *